INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 2

2021

Crimes against Women in Digital Space - In Reference to India

GOURISH GOYAL[1] AND SRINIDHI BOORA[2]

ABSTRACT

Cybercrimes are at hike and women have been drastically victimized in cyberspace. People explore themselves using the internet; they can communicate virtually, anytime, anywhere and with anyone across the world. Most women are unaware of the threats they may face in cyberspace. Some Online users known as perpetrators take advantage of it and expose women by sending obscene emails and by creating the pornographic content without their consent.

With the passage of time, many feminists fought against women violence for their empowerment in the society, but there is no end to their exploitation. The sexual offenders look for the victims on these social networking websites such as Instagram, Facebook and also on the job websites where people post their personal information for a better prospect. Due to lack of evidence and fear of defamation, identification of such cybercriminals or perpetrators becomes difficult.

A call for modernization of the preventive, conventional setup and equipped police personnel with knowledge and skills for prevention and control of cyber crimes measures were taken by our Indian parliament.

The present study highlights the cybercrimes against women in India and this paper also highlights the reasons behind the fact as why Indian women are victimized, how it's impacting their social life by combating and curtailing cybercrime against women in India.

Keywords: *Cybercrime, Women empowerment, Social Networking Sites, Cyberspace, Cyberlaw*

I. INTRODUCTION

As the times are changing criminals are opting new ways in committing the crimes. The moment when we wake up and start our day by reading the newspaper we come across many cybercrimes emerging day-by-day. The social networking sites are becoming more vulnerable to cyber-crimes like morphing the pictures, threats for sexual assaults, profile hacking, etc.

[1] Author is a student at ICFAI Law School, Hyderabad, India.

[2] Author is a student at ICFAI Law School, Hyderabad, India.

Privacy is being invaded in social media through these crimes. Cybercrimes against women in India include sexual crimes and abuses on the internet. According to data given by *National Crime Records Bureau* (NCRB) in year 2017, the cybercrimes that are reported by the women in the internet were sexual exploitation (5.1%), an insult to modesty of women (5.2%) and causing disrepute (3.3%).[3] The most important thing that is to be noticed is that not all the crimes are being reported by the victims for many reasons like thinking about the reputation, fearing the consequences. Women are becoming victims of these cybercrimes. Since the technology is changing rapidly new types of crimes are coming into existence like the "Boys locker room". There are many cybercrimes which are being committed by the younger age group people.

Recently, there was a group on Instagram which consists of school going boys from South-Delhi. They have slut-shamed and body-shamed the pictures of the girls who were younger than their age and discussed about raping them. The people have joined in the group using fake usernames and Id's. As soon as the screenshots of the chats in the group have gone viral in the social media, they have deactivated their accounts. As per the report filed by the *Delhi Commission for Women* (DCW) to the police and Instagram, the police have conducted the investigation and arrested three persons in connection to the incident including the admin of the Instagram group and a juvenile member in the group. When the screenshots have gone viral they have planned to leak the nude pictures of women and girls who were commenting on this incident. This shows that they were not at all regretting their mistake. There are many groups like these on different social media platforms. The groups like "Boys Locker Room" are becoming a new threat to the women and girls in the cyber world. Such groups are becoming a source for the commission of crimes in young minds. These groups are implanting the rape culture in the young minds by imbibing the criminal psychology.

The important question is "Are women safe on social media platforms?" The answer is no. The cybercrimes are increasing day-by-day. Cybercrimes against women are a major concern in today's world. This research paper is to analyze what are the cybercrimes against women, the acts related to the cybercrimes, the current cybercrimes that are taking place, causes and effects of these crimes, and measures for reducing the cybercrimes.

[3] Sorav jain, '7 types of social media crimes and how women should deal with it', https://www.soravjain.com/cyber-security-for-women-in-social-media/, accessed on March 8, 2018.

II. CYBER-CRIMES IN INDIA AND ITS COMBAT

According to the latest report of *National Commission of Women* (NCW) data, 54 cybercrime complaints were received online in April, 2020 in comparison to 37 complaints received in March, 2020 and 21 complaints in February, 2020.

Srivastava said on an average she has been getting 20-25 such complaints from March 25, 2020, daily while before (March 25, 2020) lockdown the number was less than 10 per day.[4]

Combat

On August 30, 2019 Cybercrime.gov.in portal was launched and it enables filing of all cybercrimes. This portal specifically focuses on crime against women, children, child pornography, child sex abuse material, online content related to rapes and gang rapes.

The above portal contains cyber safety tips, cyber awareness and a Citizen Manual which contains two pdf namely:

- Citizen Manual Report CPRGR complaints
- Citizen Manual Report Other cyber crime[5]

We will further discuss this in detail in other heading and sub-headings.

III. CYBER-CRIME AGAINST WOMEN

Cybercrimes against women is at an alarming stage. It is an offence that is committed against an individual or group of individuals with a criminal motive to defame the reputation of the victim. Women especially young girls are victimized by the perpetrators by sending obscene emails, stalking women by using chat rooms, websites etc. Indian women are not able to lodge a complaint of cybercrimes immediately.

The above problem can be resolved if women start warning these perpetrators and by reporting the crime immediately. It often creates a problem when emails and social media messages are posted using fake accounts and thus it becomes difficult to trace the perpetrator. Internet technology came into existence in 1986 but has shown immense or aggressive growth. Likewise, Radio was in existence thirty-eight years before fifty million people used it. It was sixteen years before fifty million people used a personal computer. Once the internet was made available to the general public, it took only 4 years for 50 million people to go on-line. The

[4] Susmita Pakrasi, "Significant" Increase In Cyber Crimes Against Women During Lockdown: Experts, Hindustan Times (New Delhi, 3 May, 2020).

[5] https://cybercrime.gov.in/Webform/Citizen_Manual.aspx accessed 5 June, 2020.

internet has seen to be booming, with a number of benefits but also bringing a great threat to the security of women society.[6]

This cyber violence is increasing day-by-day as an increase in online work, because the more we give our personal information to different-different websites, it directly or indirectly gets into the touch of cyber criminals who misuse such information against women. This is the reason cyber crimes against women are on the ascent.

IV. Forms of cyber offences against women

1. *Harassment via E-mail* - This form of harassment includes blackmailing, threatening, sending of love letters in anonymous names or sending of embarrassing emails. There is the Criminal Procedure Code, Indian Penal Code and Information Technology Act under which such offences and their punishment are described. Under The IT Act, 2000 Section 66 A talks about Punishment for sending offensive messages through communication service, etc and Section 67A and 67B is defined as Punishment for transmitting of material which contains sexually explicit material and Punishment for transmitting of material depicting children in sexually explicit act via electronic form, respectively. Section 67 C of IT Act deals with an obligation of an intermediary to preserve and retain such information in the prescribed manner by the central government and under section 509 0f Indian Penal Code (IPC) for uttering any word or making any gesture intended to insult the modesty of a woman.[7]

In the above cases the victim goes to the police station to file a report of harassment and under such issues any publication or transmission of obscene information in electronic form under Section 67 of IT Act, 2000 may be looked at from the perspective of 'extra territorial' jurisdiction.

2. *Cyber Pornography* - It is another type of online threat to women's security. In this Perpetrators publish pornographic materials in pornography websites by using computers and the internet.

Recently, A 38-year-old held for child porn posts on social media in Mumbai information was given by *National Centre for Missing and Exploited Children* (NCMEC) to *National Crime Record Bureau* (NCRB) and from NCRB it came into the notice of DCP (cyber) Vishal Thakur.

[6] Jaspreet Singh, 'Violence against women in Cyber world: In special reference to India' (2015) Vol. 4 'IJARMSS' 60.

[7] Shobhna Jeet, 'Cyber Crime against women in India: Information Technology Act,2000' (2012) 'Elixir Criminal Law 47' 8891.

Punishment to such offences should be given under the IT Act, 2008 under Section 67 and 67A.

Avnish Bajaj v. Union of India[8]

Avnish Bajaj was the CEO of Bazee.com website which involves the sale of property online.

It gets the income through the advertisements in its web pages. An obscene clipping named "DPS girl having fun" was kept for sale on this site. Some copies were sold through this site. The court granted bail to avnish subjecting to two sureties worth of Rs. 1,00,000/-, ordered him not to leave the country and submit his passport to the Magistrate.

3. *Cyber Stalking* - This is one of the most popular internet crimes in the modern cyber world. Cyber Stalking can be denied as continuous use of the internet and other electronic means to stalk and harass or threaten an individual or a group or individual or an organization. These cyber Stalker first stalk young girls then make threats, identify theft, damage to data or equipment and then solicitate these minors for sex or gather information and harass them.

Here the question arises what makes the cyber stalker to do such things:

Sexual harassment

Obsession for love

Hatred

Ego

Ritu kohli's case

This case has become the first case in the offence of "Cyber stalking". This is a landmark case which recognized the term "cyber stalking" and held it as an offence in the amended act of 2008. The accused (Manish) was stalking the victim (Ritu Kohli) on the internet by disguising himself as the victim and chatting on a website. He used obscene language and has given her mobile number on the website inviting the people to chat and talk to her over the phone. As a result, she received obscene calls from various people in the country and abroad. She lodged a complaint against him under section 509 of IPC for outraging the modesty of the woman. As the conditions mentioned in the section were not satisfied, the Government termed this as an offence of "cyber stalking "under section 66-A of IT Act, 2000. Through this case the offence of "cyber stalking" was defined.

[8] Crl. M.C. Appeal No. 3066 of 2006.

4. *Cyber Defamation* - It includes publishing defamatory information about the person on a website or by circulating it among the victim friends and organization.

One of the famous case of Cyber Defamation in India involving a women was *State of TamilNadu v. Suhas Katti*[9]

This is a landmark case which is related to the offence of "obscenity" in Yahoo Messenger Group. This is the first case which is booked under Information and Technology Act, 2000 and in this case the accused was convicted in the short span of time of seven months from filing the FIR. This case has been set as an example for "Cybercrime Management". In this case the e-Mails were sent to the victim through a false e-Mail account which is created by the accused in the name of the victim asking for the information which resulted in the obscene phone calls to the woman. The accused was known to the victim before the incident as he was interested in marrying her but she was married to another person and ended with a divorce. After she divorced her husband, the accused has shown interest in marrying the victim but she refused which led to the harassment on the internet. The accused was held guilty under section 469, 509 of IPC and section 67 of IT Act, 2000. He was sentenced with imprisonment for 2 years under section 469 of IPC and was charged with a penalty of Rs. 4000/-.

5. *Cyber Hacking* - These Cyber Criminals do unauthorized hacking by choosing some particular targets and accessing their computer system or network and using the personal information for evil purposes, and it is one of the most predominant forms of cyber crime. Such cyber crime takes place through social networking sites or apps like Facebook, Instagram and Orkut etc.

Morphing, hacking and email spoofing are inter-related and attracts section 43 (penalty for damage to computer, computer system etc.) and 66 (hacking of computer system; first proviso to the said section states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroyed or deletes any information residing in a computer resource or diminishes its value through alteration, its utility or affects injuriously by any mean, commits hacking) of the IT Act, 2000. According to the laws of IPC the perpetrator can be booked under Section 292A of IPC for printing and publishing grossly indecent or scurrilous matter and matter intended to blackmail and under section 501 for defamation.

6. *Cyber Morphing* - In this kind of cyber crime an unauthorised user or a person by making a fake identity on social media download the pictures of the person to whom he wants

[9] C.C.NO.4680/2004.

to make the victim and then he edit the pictures of the victim into pornographic images and upload it on the internet is known as morphing.

Air Force Balbharati School Case[10]

A student of this school got bullied by his friends for having a pockmarked face. The student got fed up by these acts and he had scanned the pictures of his friends, classmates and teachers and morphed them with the nude pictures and uploaded them in a website, then to a free web hosting service. The father of one of his classmates had lodged a complaint against the student to the police. These acts can be punished under Sections 43 and 66 of IT Act, 2000 and Section 509 of IPC.

7. Email Spoofing - In this type of cyber crime when the sender of the email forges the email header from address, so the sent message appears to have been sent from a legitimate email address. If you have received a large number of undeliverable notices in your inbox, there is a strong chance your email address is being spoofed because as you click on any link in the mail, there might be high chances of hacking. Cyber criminals often use these methods to extract personal information and private images from the victim.

Gujrat Ambuja's Executive Case[11]

In this case the perpetrator has disguised him as a woman and started blackmailing for extorting the money from an Abu Dhabi based NRI. He was charged for cheating, impersonation, black mail and extortion under various sections of IPC and IT Act, 2000.

V. CYBER LAWS

Under Information Technology Act, 2000 and Indian Penal Code, 1860 perpetrators, stalkers and cyber criminals can be booked under several sections for breaching of privacy, Email spoofing, Harassment via email, Cyber defamation, morphing, phishing, Cyber pornography and Hacking.

1. Section – 66A (IT Act, 2000): Sending offensive messages through communication services, causing annoyance etc. or sending e-mails to mislead or deceive the recipient or victim about the origin of such messages. Punishment for such acts is imprisonment up to 3 years and with a fine.

[10] Abhimanyu Behera 'Cyber Crimes and law in India' (2010) XXXI 'IJCC' 19.

[11] Gujarat Ambuja Cement And Ors. ... vs Union Of India (Uoi) And Anr., AIR 2000 MP 194.

2. Section – 66B (IT Act, 2000): Dishonestly receiving stolen computer resources or communication devices. Punishment for such offence is imprisonment up to 3 years or fine which may extend to rupees one lakh or with both.

3. Section – 66C (IT Act, 2000): Dishonestly make use of an electronic signature or other identity theft like ‘using password or unique identification number’ etc. punishment for such

act is for a period of 3 years or dine which may extend to rupees one lakh.

4. Section – 66D (IT Act, 2000): This section clearly says that cheating by caricature using computer as a resource or a communication device, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees or with both.

5. Section – 66E (IT Act, 2000): Capturing, publishing or transmitting the private area of any person without his or her consent. Punishment for such offence is three years imprisonment or two lakh rupees fine or both.

6. Section – 66F (IT Act, 2000): Cyber terrorism - Whoever intent to threat the unity, integrity, security or sovereignty of the nation and deny the authorized person to access its data or computer resource or attempt to penetrate or access a computer resource without authorization, shall be punishable with imprisonment for life.

7. Section – 67 (IT Act, 2000): The provision under this section covers the publication or transmission of vulgar material in an electronic form. The Information Technology (Amendment) Act, 2008 included child pornography and custody of records by intermediaries.

8. Section – 72 (IT Act, 2000): Punishment for breaching confidentiality and privacy - A person discloses such electronic record or register or diary or book or document or other material, shall be punishable with imprisonment for a term of 2 years or fine up to one lakh rupees or with both.

9. Section – 72A (IT Act, 2000): Breach of lawful contract by disclosure of information, with the intent to cause or knowing that he likely to cause wrongful loss or wrongful gain, without the consent of the person. Punishment for such offence is imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

10. Section – 354D (IPC, 1860): This provision of Indian Penal Code deals with stalking in all forms. It includes stalking of a woman or her contacts physically or monitoring her online activities against her consent or knowledge.

11. Section – 500 (IPC, 1860): It covers printing and engraving any matter about someone that it is derogatory and defamatory. The offence is punishable for an imprisonment up to 2 years or fine.

VI. CAUSES FOR CYBER CRIMES

Computer Knowledge

The main cause for the cyber crimes occurring in India are due to the lack of education related to the cyber crimes, and the usage of the technology. As the technology keeps on changing, one has to get acquainted with them. The other reason is the security issues in the cyber world. Most of the applications and the websites that we use are not safe. For example, the apps have access to the location, camera and social media accounts use the personal information which are easy to be hacked. We have seen that the accounts of Facebook have been hacked which led to the loss of data for the account holders. We use the unsecured Wi-Fi networks in our daily lives which makes it easy for the hackers to get the details like log- in information. As most of the women put the pictures in the social media, they can be easily morphed by the perpetrators leading to cyber crimes. There are many fake Id's which exist on social media platforms. Women can become a trap for this believing the person to be their acquaintances. The common mistake done by many of us is giving permissions to the apps without reading the terms and conditions. This results in the access to data by the perpetrators. There were no stringent laws earlier regarding the cyber crimes specifically against women like stalking, morphing, pornography, etc., which resulted in the increase of cyber crimes.

Sociological Reasons

In this 21st century which is known as 'digital book' still in India there are gender and caste differences. In India society decides the role of both men and women. Till now in many villages people think men are bold, serious, dignified, responsible, unemotional and dynamic so, they should go out and work and learn new technology whereas women should do household work as they understand, emotional, patient and compassionate. Due to this, these women don't know the proper use of technology and it eventually leads to an increase in cyber crimes.

Many cases of cyber crimes are not reported until today due to fear of defamation of family's name, threats by the perpetrator, shyness and fear etc. In some cases a woman thinks that she is responsible for the crime that happened to her. Many times women feel that their friends, family do not support them and instead question her for that. In most of the cases the victims are being blackmailed by the perpetrators for extorting the money, not approaching the police for a complaint. Women feel insecure when they are being victimized by the people. Due to these fears the victims do not take any action against the perpetrators which encourages them to do crimes against the other victims, causing the increase in crimes.

VII. Effects of cybercrime on victims and society

Cybercrimes have an emotional impact on women and individuals. About 80% of the victims do not want to report the crime due to the helplessness, shyness and fear about her and his family reputation. The question arises in the mind of the victim whether or not they will get support from their family members or friends. When the crimes are not being reported by the victims the perpetrator may commit the same crime with others leading to an increase in the crime rate. The victimization by the friends, parents, family and society may lead to anger, depression, fear, shock in the victims. The victims need to overcome these problems. It takes a lot of time to get out of these problems by the victims. They face many challenges during this time. At this stage the victims may also have suicidal thoughts.

As we have seen cases like cyber bullying and boys locker room incidents, the perpetrators who commit such crimes are of younger age. Basically, the younger people are psychologically turning to be the perpetrators. The cyber-crimes are being committed irrespective of the age groups which are impacting the society. These are the ill- effects of cyber-crimes not only on the victims but also on the society as well.

VIII. Measures to overcome cyber criminals

1. Awareness campaigns should be brought up by the government, schools, colleges and NGOs and make the students understand or aware of various forms of cyber crimes such as cyber stalking, cyber defamation, cyber harassment via email, cyber hacking, email spoofing, morphing and phishing.

2. By changing passwords from time to time of all their social media apps including software and Gmail, bank pass code, credit card etc. this will keep the cyber hackers away from our personal data. Safest password is a password which contains letters, numbers and symbols, and everyone must try to maintain that type of password, as it will be tricky for any person to break. The most important point that keeps your mobile phone password protected.[12]

3. Avoid giving phone numbers to the people whom you just met or to the person about whom you don’t know properly. It can be used as cyber harassment by the perpetrators. Through latest tech they will first search your number on internet, then they will get your name

[12] Jaspreet Singh, ‘Violence against women in Cyber world: In special reference to India’ (2015) Vol. 4 ‘IJARMSS’ 60.

and then they will make a fake id and will try to connect to you and then try to steal your personal information and this will lead to Cyber pornography and morphing or your pictures and personal information.

4. Avoid giving residential address; especially the women who are running businesses or women in a professional field are very visible to the general public. They can use a work address or rent a private mailbox. It helps them to avoid cyber stalkers. Moreover a woman should not post more personal information on social networking sites as it can be seen by the public at large and can come into the contact of cyber criminals.

5. Seminars and workshops should be conducted for better understanding of cyber threats. In these seminars not only the students but also the police, lawyers, NGO, government officials and social workers must be invited to discuss legalities and illegalities of cyber crime. Special seminars should be conducted for police officials for better understanding of such kinds of victimization and better understanding in combating and giving quick responses to the complaints.

6. Laws should be made more stringent for cyber crimes against women in digital space. The Information Technology act contains only a few sections of cyber crimes and that also for women. So IT Act must be modified to such stringent laws that cyber criminals would be afraid of doing cyber crimes.[13]

7. With the help of NCRB and app making officials such websites and apps should be developed where an immediate action can be taken by both the victim and the police to curb the cyber crimes. This will help to reduce cyber crime. Forensic Laboratories should also keep them updated with all the latest equipment required to solve a case of cyber crime.

8. Always read terms and conditions before installation of any app or software. It sounds useless and plus in this modern and fast world no one has that much time to read terms and conditions of every software or app they install, but here's how it helps. Some websites have the legal rights to own, share, sell or resell your personal information to anyone they wish to. If defrauded on such platforms after agreeing to their policies, even the law cannot help you get justice.

9. Never leave your webcam connected and block unwanted people – Make sure that you disable your webcam when not in use. For laptops we recommend applying a sticker or tape to cover the webcam when you don't need it. Whereas many times you have noticed that you

[13] Abhimanyu Behera 'Cyber Crimes and law in India' (2010) XXXI 'IJCC' 19.

receive spam or fake calls, but people don't care about it and keep it in your mobile phones without blocking it, but here the twist. As you pick up the call or don't block these spam calls after you answer them wrong number, they can hack your mobile phones and steal your private data.[14]

10. Always keep the security system update of your mobile phones, computer and laptops.

Installing genuine anti-virus software will help you protect from the cyber hackers. Make sure that your system firewall is up-to-date against malware and malicious software.

IX. Critical Analysis

Cyber crime is an illegal activity done by cyber criminals and the primary source of that crime is the internet and computer. Women are the main victims of cyber crimes and these cyber crimes include cyber hacking (the base of all crimes), cyber stalking, cyber harassment, cyber pornography, and morphing, phishing and cyber defamation. Laws are implemented by the government of India regarding cyber crimes and those laws are mentioned under Information Technology Act, 2000.

Mostly young women and girls are the victims, as they don't know the proper use of technology and without understanding the terms and conditions they one by one install social media apps such as Instagram, Facebook, Tik Tok and many more and start uploading all their private information on these social media apps. These hackers by making anonymous accounts in the names of the victim's friends collect images and all private information from the victims and start harassing them, sending obscene images or their pics and also by threatening them.

These young women and girls should be made aware by the government, police officials, institutions, NGOs, parents and by their friends. By giving education about laws available and measures to overcome these cyber criminals, measures such as changing password of social media apps and of the phone on a regular basis. Avoid giving mobile numbers and residential address to the unknown or to the people whom you don't know properly. Victims should immediately report the crime to the police or through the apps available without and fear of family members.

All the above necessary steps and measures should be kept in mind by the victim to stay away from the causes and effects of these cyber crimes. Non performance of above measures will lead to increase in cyber crimes. Otherwise it will lead to lessen cyber crimes by the

[14] 'Online Harassment and Cyber Crimes against Women – An Insidious Menace' (January 24, 2019), https://www.ardcindia.org/online-harassment-and-cyber-crimes-against-women/.

perpetrators, if proper measures and steps are taken by the victim on time and at last it will lead to betterment of women and young girls in the society at large.

X. Conclusion

The main element in the cybercrimes is the "Modus Operandi". Every crime is made differently by the perpetrator. The investigating authorities, judicial system should have the knowledge of the latest technological developments and make sure that justice is served to the victim. The laws should be updated as per the changes in the technology and crimes. If necessary, new laws and amendments should be made in the parliament for security of women in the cyber world. While framing of the constitution, the framers were not aware of the technological developments that have taken place over the years. So the laws should be made strict keeping in view of the crimes. As the perpetrators are increasing there is a need for people like "ethical hackers" to detect the crimes. The universities should have special courses regarding the subject of Ethical hacking. Women should be aware of the cybercrimes that may take place and take the necessary measures to reduce the risk of falling into the trap of perpetrator. The victims who are affected due to these cybercrimes should not be victimized but rather they should be supported by the society. The victim should be strong and report the crimes fearlessly.

The education system should be changed and students should be imbibed with morals so that they don't turn into perpetrators and the victims can protect themselves from these cybercrimes. There are many apps like cyber security app, cyber crime clinic, cybercrime helpline. These apps should be made use of properly. The apps like these are to be invented to create awareness among the people regarding cyber crimes. The victims may go through the psychological problems like "*Post Traumatic Stress Disorder*" (PTSD), suicidal thoughts, trauma, and other problems. They have to get the help from the psychologists regarding this and be brave. As women are more vulnerable to cyber crimes, they need to be given awareness and training by the NGOs, educational institutions and other organizations regarding the occurrence of cyber crimes and safety measures to combat these types of crimes. Most of the cybercrimes that are committed against the women, the perpetrators have turned out to be the known persons to the victims. Women should take the necessary safety measures on social media platforms and internet spaces. Moreover, the government has to introduce the subject on cybercrimes, its effects, and measures to be taken by the individuals in the schools at secondary level so that they have the awareness about these crimes and take the necessary steps in the future. We should educate the people to report the cybercrimes without any fear, so that the perpetrator gets punished for his acts.

The cybercrimes against women can be countered only with the reforms in the laws as per the changing technology and changes in the education system. In India, the stereotypic mentality exists that women are not on par with the men. This mindset should be changed. Women should be encouraged by society to report the crimes fearlessly instead of victimizing them. These changes cannot be done in a single block of society but the people, government, judiciary needs to work together in bringing these changes.

*****