Page 1888 - 1902

DOI: *https://doij.org/10.10000/IJLMH.116320*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

Victimization of Women in Cybercrime: An International Perspective

VISHAKHA TYAGI[1]

ABSTRACT

Cybercrimes against women are increasing and women have been severely victimized in cyberspace. Some criminals try to offend women by sending obscene e-mails, stalking women through chat rooms, websites, etc., developing pornographic videos that present women in compromise, mostly created without their consent, fraudulent e-mails, images that turn into pornographic content, etc. Sex offenders look for their victims on social networking sites as well as job or matrimonial sites where people post their personal information for a better future. Disclosure of personal information has made women increasingly victims of cybercrime. Although there are many cases of female victimization in western countries, female victimization has increased in eastern regions such as India, and these women have relatively less legal protection and are unique than their western counterparts (Halder and Jaishankar), 2008, 2009, 2011b). This article attempts to explore the various reasons why Indian women have been victimized and proposes a conceptual model of Indian women's cyber victimization.

As victims of cybercrime, women experience a number of psychological effects that deeply affect their lives. The National Crime Records Bureau (NCRB) has reported an increase in cybercrimes against women in recent years. Cybercrime against women takes the form of online defamation, sexual harassment and abuse, email spoofing, etc. This research paper is an attempt to discuss a brief analysis of women's legal rights to protect themselves against cybercrime, its implementation and the challenges women face in achieving these rights.

Keywords: *Cybercrime, Regulations, Law and Policy, IT Act 2000, Technology.*

I. INTRODUCTION

Cybercrime is a global phenomenon. Women have been victims of various types of harassment for centuries and until now. Domestic violence, Sathi Paratha, acid attack, rape, bullying, sexual harassment, dowry, harassment, kidnapping, honour killings, female infanticide, etc. are some of the categories of violence against women. The brutal rape death of a 23-year-old paramedic in New Delhi last December drew attention to violence against women and for the first time sparked widespread protests among Indians across the country who raised their hands against

[1] Author is a LL.M. Student at UILS, Chandigarh University, Mohali, Punjab, India.

the violence. against women in India. The United Nations defines violence against women as any gender-based violence that causes or may cause physical, sexual or mental harm or suffering to women, including the threat of such acts, coercion or arbitrary deprivation.

Acc. to Swapna Majumdar: "Violence against women is not cultural or regional; it involves community and class. Although shocking, the fact is that violence against women has become an accepted norm of life because women accept violence as part of their marriage until it becomes intolerable. (Majumdar 2003). We all celebrate International Women's Day every year on March 8 to show our respect, love, affection and appreciation to women for their economic, political and social achievements in various fields. Even in India women are worshiped as goddesses (Devi), Kanya, Mata etc.) but the reality shows a darker and deteriorating picture of it. Actually, women are worshiped only in religious places or religious programs or festivals but in common life they are used in many ways and always were victims of physical, psychological, sexual abuse etc. India has become the worst place in the world for exploitation of women. It feels proud because it is considered the world's largest democracy, but the recent gang rape of a woman running in a bus in Delhi, abuse of a woman, dowry harassment, dowry death, harassment, kidnapping, domestic violence, female infanticide, honour killings. cyber violence etc. reveal the true picture of India, how difficult it is for women life in Indian democracy. Equality of all was mentioned in the preamble of Indian constitution e.g. "To secure to all its citizens social, economic and political justice, freedom of thought, speech, religion, belief and worship; equality of status and opportunity; fraternity that guarantees the dignity of the individual and the unity of the people. In the aforementioned law, certain crimes are classified as punishable crimes, such as hacking, publishing obscene material online, data manipulation. Safe environment offers to parents to improve their children's online safety. Both technical measures to protect computer systems and legal measures to prevent and prevent crime are implemented. Cyberspace is a new horizon driven by machine data and any criminal activity that uses a computer or network as a source, tool or target is called cybercrime.[2] Cybercrime against women in India is a new concept. When India started its IT journey, the protection of e-commerce and communications under the Information Technology Act, 2000 was paramount, while cyber-data communications remained untouched. It used to be limited to roads or places away from home. Home was the safest place for a woman to protect herself from victimization, but not now. Home becomes for them an equally dangerous place, prone to criminals. However, the limit will be set on their computer screens. This is a serious concern. The increase in cybercrimes against women has led to insecurity among women. They don't know nowhere is

[2] Desai, M. and Jaishankar, K (2007). Cyber Stalking-Victimization of Girl Students: An Empirical Study.

safe anymore. Its impact on them and society as a whole is greater when looking at the bigger picture. Today, in this globalized world, we are surrounded by various man-made inventions our life is simple and comfortable. One such great invention of mankind is the Internet. From online shopping to collecting Due to the rapid development of the cyber world, information is now so easy and accessible. One can you can get information on any topic in minutes. Easy access to computers and things on the Internet is rapidly changing around us, from communicating with friends and family to studying and working online the feeling of home seems so accessible to all. It has become a part of our lives. Besides, we all are depend on internet for every little thing. Cybercrimes such as cyber terrorism, identity theft, it targets phishing emails, data breaches, privacy breaches, fraud and other computer-related crimes.

(A) Concept of cybercrime

The industrial revolution opened the way to modernization and technological development. Together as technology has evolved over time, it has gradually changed the settings of the entire society. But the biggest cyber development contributed by the INTERNET. It has become part of our daily needs. But eventually it became a platform to commit crimes. People started abusing this great invention. The development of the Internet in the cyber world brought a drastic change in the modernization of the world, but even opened doors side effects This gave birth to what we now call "CYBERCRIME". Today every third person has been a victim of some sort of cyber abuse. It has spread its roots all over the world whether you talk about developed nation or underdeveloped nations. The cybercrime poses threat not only to individual but even to national security and the citizens of the nations. In the growing trend of using smart phones and being active on social media sites one must not forget that apart from being an entertainment platform, it poses a threat of cybercrime as well. But in most of the cases it is seen that the cyber criminals always look towards new methods to attack the individual either for his own interest or for the sake of entertainment. This can be done against anyone without even knowing that we have fallen victim to it. Like today, when everything is digitized, it changes it is easy for a criminal to target a person and commit a crime against them.

(B) Objective of this study:

- To study the concept of cybercrime against women.
- Female insecurity increases cybercrime.
- View all laws regardless of whether traditional or modern technology means.
- To study the existing legislation on cybercrime in India and find out whether it exists are adequate to fight cybercrime or there are loopholes in existing laws

- To finds out the problems of women in reporting crime and other causes of crime fewer convictions for cybercrimes against women.
- Explain the steps regulatory agencies must take to analyse crime against women.
- Need for effective intelligence apparatus to fight cybercrime against women.

(C)Types of Cyber-Crimes against Women

Basically, cybercrime is any illegal activity that uses a computer as the main means of execution. It has been expanded to include activities such as crime on the Internet, crime related to the Internet, violation of Internet laws, illegal activity through the Internet, violation of the Internet Act, computer crime, violation of any law through the Internet. Internet, Internet corruption, Internet criminal activity, Internet malware, electronic crime, Internet crime, Internet smuggling, Internet stalking, Internet identity theft. Cybercrimes can be committed against persons, property and government. The most common types of cybercrimes are discussed below.

- **Email Bullying**: This is not a new concept. It is very similar to bullying. This includes blackmail, threats, harassment and even email fraud. Although e-bullying is similar to letter bullying, it often causes problems when sending fake IDs. Harassment includes blackmail, threats, harassment and email fraud. The Criminal Law Amendment (Bill) 2013 was recently drafted under the Indian Sexual Harassment Act. It defines harassment as physical contact and advances that include unwanted and explicit sexual overtures.
- **Cyber stalking**: This is the use of the Internet to abuse or harass someone online. A cyber stalker does not physically harm the victim, but monitors the victim's online activities to gather information. Uses verbal threats to threaten the victim. A study of 72 women by Megha Desai and K. Jaishankar found that 12.5% of those surveyed were intimate with their cyber stalker before the stalking began. The Ritu Kohli case was India's first cybercrime case. In this case, Mrs. Ritu Kohli has complained to the police about a person using her identity to chat on the Internet, mostly on a Delhi channel, for four consecutive days. He also complained that the person chats online, uses a name and speaks obscene language. The same person also gave his phone number to other chatters and asked them to call Ritu Kohli. He received almost 40 calls from unknown numbers. The IP address was traced and the whole matter was investigated by the police and eventually the criminals were arrested. Section 72 of the Information Technology Act

covers laws relating to cyber consequences. It says that the preparation can be ordered far admiring the modesty of the women.

- **Cyberpornography**: Cyberpornography refers to the use of cyberspace to create, display, distribute, import or publish pornographic or obscene material, especially material depicting sexual activity between children and adults. Cyber pornography is a crime classified as causing personal injury. A very famous case of DPS MMS scandal was reported under this type of cybercrime. In this case, an MMS clip was made by a schoolboy in a dangerous situation, which was distributed among different networks. In several other cases, video clips leaked through CCTV recordings are very popular. Section 67 of the IT Act, 2000 covers cases of cyber-porn. According to this law, the perpetrator of the act can be punished under a different section of the criminal code.
- Section 290 on public nuisance.
- Section 292 on obscene sale of books etc. Impact factor: 4.819
- Section 292A which deals with printing or publishing grossly indecent or malicious or deceptive material.
- Section 293 for sale of obscene articles to minors.
- Section 294 for making or composing, writing obscene songs etc. and
- Section 509 to outrage the modesty of women. Women are easy targets for any type of cybercrime. With more than 560 million Internet users, India is the second largest online market in the world after China, according to research. Studies have also reported that by 2020, 40% of women will use the Internet. Among the states of Kerala, Tamil Nadu and Delhi, the percentage of female internet users is higher. Expert reports have also said that cybercrimes against women, especially sexual harassment, have increased significantly during the COVID-19 lockdown, with "cage criminals" targeting them online.
- **Cyber defamation**: Cybercrime including defamation, is another common online crime against women. This occurs when defamation is committed via computers and/or the Internet. For example, someone posts defamatory material on the website or sends emails containing defamatory information to all of that person's friends or relatives. This is mostly done by hacking someone's Id on Face Book, Google or any other social network or post office. This is also done by creating a fake profile of a person that contains all the personal information that looks authentic to others on any website.

- **Morphing**: Changing the original image by an unauthorized user or a false identity is called morphing. Fake users have been found uploading photos of women and reposting them on various websites, creating fake profiles after editing.
- **Email spoofing**: An email that misrepresents its origin is a fake email. That shows its origin different from the actual origin.

II. Impact of cybercrime

In this age of technological progress, women are the most victims. Every phase of life today begins and ends with digital interference, with computer-technical interruptions. In the light of this, there are also positive and negative aspects. Cybercrime is a global phenomenon. The development of technology, cybercrime and victimization of women is rapid and poses a great threat to the safety of the whole person. This growing cybercrime in the cyberspace threatens the privacy and security of an individual. The Internet is the world's largest information system and a gigantic network. As the development of telecommunications infrastructure continues to penetrate into smaller cities, the figures on internet usage show the impact of this ever-growing number of users. Cyberspace has been a boon to human civilization. The Internet has connected people all over the world. The desire to know the unknown is essential to human nature. It is the desire to get to know the people living on Earth that feel the need to find a way without human traffic. This led to the discovery of the cyber world.[3]

- Social networks have developed a new way for interactions & meetings.
- Despite all the problems, women in the society are fully satisfied with this liberty.
- From online shopping to E- Transaction of money made life easier for women.
- Internet works as a blessing but on the other hand it has made the life of women insecure due to increasing cybercrime in the virtual world.
- With the arrival of the Internet, privacy of women’s as at risk by using social media platforms.
- India is mainly a patriarchal and orthodox country and women victims are mostly guilty and internet, victims have no exception.
- The spread of information and communication technology offers great opportunities and more ways to connect.

[3] Fabiu Marturan, Simone Tacconi and Giuseppe F. Italiano (2013) cybercrime and cloud forensics: Application for investigation process (pp.313-3300)

- The price for using gadgets & Internet devices also contributed to the growth in problems.
- The increase in ICT penetration has accelerated the growth of ICT-based businesses and services.

Impact of Cybercrime on mental health

According to the National Crime Records Bureau (NCRB) Crime in India - Statistics Volume II, a total of 10,405 cybercrimes against women were reported in 2020. From online blackmail, online stalking, defamation and mutilation, women are the target of a number of online crimes, and deception. Thus, approximately 1,102 cases of children were registered in 2020. There are social and psychological effects on a person who faces cyberbullying, stalking, harassment, etc. As a mother, it is even more important to consider the change in the behaviour of children if they suddenly become poor in the academy, become isolated, avoid going out, meet friends or even be on the Internet and suddenly violent behaviour. It is important to keep the communication channel open with the children, and when such a case is discovered, the mental rehabilitation of the affected children is as important as filing a complaint.

III. Legislative provisions

Providing a safer platform for women to use the Internet is becoming important Government is drafting effective legislations to prevent all crimes against women in cyberspace a room. In this regard, India has such laws to protect women from falling in the hands of cybercriminals. The Information Technology Act of 2000 is one such important law which protects the interest of women and protects against all cybercrimes. From The Indian Penal Code and the Constitution of India provide for the safety of women.

These statutes or statutes lay out the procedures to be followed when dealing with cyber matters criminal cases but unfortunately after we have laws to protect women from cybercriminals cybercrimes against them have increased. The reason for this situation is that we do not have a uniform a code that specifically addresses cybercrimes against women. This is the need of the hour for formation an effective legal system that strictly controls all malicious activities in cyberspace for women and provides a safer platform for women to use cyber technology. We need effective and a time-saving mechanism to combat the victimization of women in the cyber world and provide them an atmosphere where they can grow and develop their personality without obstacles. This research paper deliberately tries to define cybercrime against women and the reason why women is mostly aimed at the cyber world. This further emphasizes the effectiveness of existing legislation fight the victimization of women and make some recommendations to protect them from cybercrimes crimes It explores the various methods that can be adopted by the government to control the cybercrime against women.

Indian Constitution and cybercrime

The right to privacy is an important natural need of every human being. The right to privacy prohibits interference with others and their private lives. The Supreme Court of India has clearly stated in its judgments that the right to privacy is part of the fundamental right guaranteed by Article 21 of the Constitution of India. Invading someone's privacy or stealing someone's intellectual work or information completely violates their privacy.

Position of Indian Law

In India, cybercrime is addressed through the Information Technology Act, 2000, and its amendments. This law provides a legal framework for dealing with offences related to the Digital Contracts, Digital Property and Digital Rights Act including unauthorized access, data breaches. Hacking, and online fraud. This act provides very high penalties for cybercrime.

The Indian Penal Code (IPC) and other statutes may be invoked to address specific cyber offences. The government has established agencies like the cyber crime cells and the cyber crime investigation units to investigate and combat cybercrimes.

In case of damage to a computer, computer system or computer network caused by the spread of a virus, denial of service, etc., the victims can be compensated up to five million rupees. Although India is one of the few countries that have enacted an IT Act, to fight against cybercrime, but women issues are still untouched by this law. As can be seen from the preamble of the law, it broadly covers economic and commercial matters IT Act, 2000.[4]

IT (Amendment) Act 2008, section 67 (A) (B) (C). Information Technology Act 2008, Ministry of Justice, Justice and Business Affairs (Legal Section). Published in www.manupatra.com Articles Section of Bharati Law Review, April-June 2017 New Delhi Police arrested Manish Kathuria. He stalked an Indian woman, Ms. Ritu Kohli, illegally chatting on MIRC in her name, used obscene and offensive language and shared her residential phone number, inviting people to talk to her on the phone. As a result, Ritu kept getting obscene calls from time to time and people would immediately talk obscenities with her.

Dr. L. Prakash Vs. Superintendent: In this case, the accused was an Orthopedic who forced women to perform sexual acts and then uploaded and sold the videos as adult entertainment around the world. He was charged under Sections 506, 367 and 120-B of the IPC and Section

[4] The Information Technology Act 2008, Ministry of Law, Justice and company affairs (Legislative department).

67 of the Information Technology Act, 2000. He was sentenced to life imprisonment and a fine of Rs 1,25,000 under the Immoral Traffic (Prevention) Act, 1956.[5]

State of Tamil Nadu Vs. Suhas Katti: In this case, the accused posted inappropriate, defamatory messages about a divorced woman in Katti's yahoo message group and advertised her as a sex lawyer. This case is considered to be one of the first cases where both cases are punishable with imprisonment which may extend to ten years and fine which may extend to two lakh rupees.

- Cybercrime against victimization of women is a topic that few talk about, that little is dealt with and huge victims suffer helplessly.
- India is used to describe online sex crimes and sexual abuse, such as changing one's image and using it in pornography, harassing women through blackmail or online violence.
- The nature of sexual crimes.
- Eve scoffs.

IV. International perspective

(A) In UK

The recognition of sexually sensitive cybercrimes as a potential threat to society only began in the late 1990s in Great Britain, when the stalking of female celebrities via the Internet began to be widely discussed in the media (Ellison and Akdeniz, 1998). In practice, the UK cybercrime investigation scenario is moving more towards the analysis, including legislation, of cybercrimes targeting national security, financial security, corporate identity, information and child safety. Cyberbullying and crimes against women are dealt with in depth in the Harassment Act 1997. Compared to the US, the UK setting is more conservative in regulating gender-based cyber-bullying, except for harassment involving physical harm.

Cyberspace rules to protect women UK. This chapter describes various aspects of UK cyberspace regulation. Provisions for unauthorized access and related activities, stalking and stalking, sexually offensive communications and sexual offenses are detailed. In addition, consensual and non-consensual sexual exposure on the Internet and various related regulations are analysed. A debate is followed emphasizing the creation of new women-centric laws to protect them in cyberspace as existing laws on crimes against women in cyberspace are found

[5] Dr.L. Prakash V. Superintendent (Madras High Court, W.P. 7313, 2002)
Tamil Nadu V. Suhas Kutt, 4680 of 2004 Criminal Complaint.

to be archaic. This is made clearer by the available UK cybercrime statistical reports. Analysing the 2008-2009 "Garlik", "The Internet experts"1 report from 2011, it can be observed that there are approximately

2,374,000 cases of online harassment among the 29. 7 million adult Internet users in Great Britain. In the case of online harassment, the report points to emotional suffering of the victim, persecution, unwanted, sending hateful, violent messages, racist messages, threatening messages, blackmail messages, etc. This report shows that among other crimes there were 86,900 cases of identity theft and identity theft. fraud (which involves impersonation), using another ID card, identity theft, etc. mainly for financial gain),4 207 700 financial frauds (including lost plastic cards, bank frauds, etc.),5 137 600 cases of computer abuse (the report does not include virus infections). 609,700 sexual offences, which mainly involved child victimization. Apart from the Garlick report, we could not find a detailed analysis of cybercrimes, especially against women in the UK. This may indicate how people, especially women, are conservative in reporting cybercrimes that happen to them. A victim survey to identify online crimes against women in the UK is the need of the hour.[6]

Here are some key aspects of women becoming victims of cybercrime in the UK: **Online harassment and exploitation**: Women in the UK, as elsewhere, face online harassment and abuse on social media platforms, forums and other online spaces. This can include trolling, threatening messages and spreading false or harmful information. **Cyber chat**: Cyberstalking is a form of harassment that involves the use of electronic communications to stalk, track or harass a person. Women can be targeted by cyberbullies who invade their privacy and use digital tools to intimidate or control them. **Revenge Porn**: The consensual sharing of intimate images, commonly known as revenge porn, is a type of cyberbullying that can cause serious harm to women. Offenders may share explicit images without victim consent, resulting in emotional distress and potential damage to their personal and professional lives. **Identity theft and online fraud**: Women in the UK can also fall victim to identity theft and various online scams. Cybercriminals can use stolen personal data to commit financial fraud or engage in other criminal activities.

Online dating scams: Online dating scams, where criminals create fake profiles to create romantic relationships and then benefit victims financially, could be targeting women in the UK. Information campaigns and education are important for people to recognize such scams

[6] cybercrime and the Victimization of women Law Rights and Regulations; Accessed on 25/11/2023. Available at; https://www.researchgate.net/publication/278015875

and avoid falling victim to them.

Legal protection: The UK has laws dealing with cybercrime and cyberbullying, including the Malicious Communications Act and the Communications Act. However, there are still problems in the actual implementation of these laws, and efforts are being made to strengthen the legal protection of victims.

Support services: In the UK, support services and helplines are available to help victims of cybercrime, including because of their gender. These services provide advice, emotional support and resources to help victims cope with the consequences of cyberbullying.

Education and awareness: Increasing awareness of digital literacy, internet safety and the potential risks associated with online activities is critical to preventing victimization. The training initiatives aim to empower people to protect themselves and recognize the signs of potential cyber threats.

Efforts by law enforcement, government agencies, not-for-profit organizations and technology companies are essential to create a safer online environment and prevent women becoming victims of cybercrime in the UK. Addressing this complex and evolving problem requires continued collaboration and a multifaceted approach.

(B) In USA

The United States has seen the rapid growth of the Internet and the subsequent explosion of cybercrime. The new millennium has also seen an increase in cybercrimes against women in the United States. According to WHOA 2000 statistics1, out of 353 respondents, 87% of cybercrime victims were female and 68% of bullies were male and only 27% of bullies were female. According to these statistics, victimization most often began via e-mail (39.5%), message boards (17.5%), and also chat rooms (15.5%), excluding instant messaging (IM) or a website. WHOA statistics from 2009-2010 show that of the 349 respondents, female victims continued to be the majority, accounting for 73 percent of the victim proportion. Only 27 percent of men reported being harassed. The statistics showed that 44.5% of the bullies were men and 36% of the bullies were women. The main centre of crime continued to be e-mail communication (34%); followed by instant messaging (IM), chat rooms, etc.2 The terms and conditions of the Internet service providers hosted by the United States3 emphasize the fact that the freedom of speech and expression guaranteed by the First Amendment is on the websites (Citron, 2009b). Various literature reviews show that the development of various cybercrime laws in the United States has been characterized by huge disputes about the likely clashes and confusions of constitutional rights. One law after another was created and their practical utility and constitutionality debated publicly, some withstanding the acid test of legal accountability by the Supreme Court, some not. However, none of them are designed solely to protect women's interests online. In the next section, we will analyse the applicability of current criminal laws to prevent the victimization of women on the Internet.[7]

The victimization of women in cybercrime is a serious and complex problem in the United States and around the world. Cybercrime can take many forms, including online harassment, cyberstalking, revenge porn, identity theft, online fraud, and other forms of digital abuse. Women can be disproportionately targeted in these activities and the impact on victims can be significant. Some of the key aspects of cybercrime victimization of women in the United States include:

Online harassment and exploitation: Women often experience harassment online, which can range from offensive comments and trolling to more serious forms of cyberbullying. This bullying can take place on social media platforms, online forums and other digital spaces.

Cyber chat: Cyberstalking is the use of the Internet or other electronic means to stalk or harass a person. Women can be targeted by individuals who infiltrate their online environment, monitor their activities and use digital tools to intimidate or control them. **Revenge Porn**: Sharing intimate images without consent, commonly known as revenge porn, is another form of cyber use that disproportionately affects women. Offenders may share explicit images without the consent number of the victim, causing emotional distress and potential damage to their personal and professional lives.

Identity theft and online fraud: Women can also become victims of identity theft and various online scams. Cybercriminals can use stolen personal information for financial fraud or other criminal activities.

Online dating scams: Women are often the target of online dating scams, where criminals create fake profiles to create romantic relationships and take financial advantage of victims.

Inadequate legal protection: The legal framework to combat cybercrime against women is constantly evolving, but there are still challenges to ensure adequate legal protection. Laws and law enforcement practices may not always keep pace with rapidly changing cyber threats.

Effects on mental health: The emotional and psychological impact of cybercrime on women can be severe. Victims may experience anxiety, depression, and other mental health problems

[7] cybercrime and the Victimization of women Law Rights and Regulations ; Accessed on 25/11/2023. Available at; https://www.researchgate.net/publication/278015875

as a result of cyberbullying.

Governments, law enforcement agencies, defence groups, and technology companies are all working to address and combat cybercrime. Public awareness campaigns, digital security training and improvements to online platforms and; security measures are an integral part of these activities. Fostering a culture of respect and responsibility online is essential to reducing women's victimization of cybercrime.

V. JUDICIAL DECISIONS TAKEN AGAINST CYBERCRIME CASES

In India, the judiciary is considered the most important wing of the government, helping to interpret laws, resolve disputes arising in courts and provide fair and just justice. As society changes, so do the crimes, and in order to understand the nature and severity of the crime, the judiciary must stay abreast of the further development of technology. The huge increase in the number of cybercrime cases has changed the scope of the judges in dealing with cybercrime cases. There have been various decisions in cybercrime cases that have helped change the Various judgments have been passed related to cybercrime cases, which has helped to change the perspective and has encouraged special training in laws relating to technology and computer networks, to be imparted to the judicial officers, prosecutors, and police officers, in delivering speedy judgment for the purpose of serving justice.

Ritu Kohli Case - This is the first cyberbullying case reported in India where a person named Manish misused the identity of Ritu Kohli to chat online using her name, giving her address and phone number to strangers in the chat room and encouraging them to call and provoke by speaking very foul and offensive language on the website for four consecutive days. In the first three days, he received almost 40 calls. This damaged his personal life to a great extent. later he reported the whole matter to the police and the police started an investigation and found the culprit. Apparently, a case has been registered under Section 509 of the IPC to outrage Ritu Kohli's modesty.

State of Tamil Nadu v. Suhas Kutti C No. 4680 of 2004- Under the Information Technology Act, 2000 this case was the first leading conviction case in India where the accused was convicted within 7 months of hosting the FIR. In this case, the victim was a divorcee who was constantly harassed by the accused, who later turned out to be a friend of the victim's family and was interested in marrying her. the accused created a fake profile of the victim in her name and posted her phone number on several other social media sites. The accused was charged under Section 67 of the IT Act, 2000.

VI. Suggestions and steps to tackle cyber crime

Change passwords from time to time: In fact, we all love to easily remember passwords because it is easier. If you want to reduce the risk of online crime, changing your password is a great way to make personal information and social networks safe and difficult for cybercriminals to access (Pennelli 2012). A confusing or complex password protects all accounts, including cell phones, email, landlines, bank accounts, credit cards, etc., and is difficult to guess. Even secret questions should not be answered easily (Moore, 2009). The most secure passwords contain letters, numbers and symbols. Avoid dictionary words and important dates that require different passwords for different websites (Online Privacy and Security Tips 2010). But changing your password can be very helpful in protecting your privacy.

Avoid revealing home address: This rule applies especially to women who are business professionals and are highly visible. They can use a work address or rent a private mailbox. Thus, it can help them avoid cyber stalkers (Moore 2009). In addition, women should avoid uploading a large amount of their information to the Internet so that no one can easily access it.

Maintain stable social relationship: There's also the fact that we all want to believe we should have 2,000 friends. Dunban's number refers to the limit of the number of people with whom a person can form decent social relationships, and that number is 150. We probably don't need those 2,000 Facebook friends because we probably won't know more physically. more than 150 of them limiting the number of people ensures that our information is shared with people you really know and away from friends of friends you don't know very well (Pennelli 2012). Women should stay away from unauthorized friendships.

Cybercrime Awareness Campaign: Awareness campaign should be created at grass root level like schools, collages etc. on cybercrimes such as stalking scams, financial scams, defamation, misuse of e-mail websites and social networks, virtual rape, cyberpornography, e-mail scams, etc. (Halder and Jaishankar 2010: 22). These campaigns can be fruitful in harming cybercrimes.

Seminars and workshops to better understand cyber-victimization: Police, lawyers, social workers and NGOs should be invited to educational institutions, clubs, corporate offices, awareness campaigns, seminars and workshops to discuss the legality and illegality of cyber-behaviour adults, including both sexes. Direct reporting of cybercrime victims to the police and NGOs at all levels should be encouraged. Second, workshops and seminars must be organized for police officers to better understand this type of victimization and respond quickly to complaints. Academic and legal experts, non-governmental organizations, etc. should be invited to such workshops and seminars (Halder and Jaishankar 2010: 22).

VII. Conclusion

Crime against women is not a new thing in India and especially cybercrime has added a new chapter to it. In the 21st century, when a new digital world is born and the internet has become an important part of an individual's life, cybercrime is threatening and dangerous for the safety and dignity of women and also for society. It violates women's right to privacy. The more time women spend online without knowing the pitfalls of the Internet, the more vulnerable they become. The consequences of cybercrimes are extremely dangerous in all forms, be it cyber stalking, harassment, defamation etc. The increase in cybercrimes against women is a major concern for the judiciary, the government and society as a whole. The after effects of cybercrime are very threatening and dangerous to the mental and physical health of the victims. It causes a lot of suffering to women, which even leads to suicide if not treated on time. Cyberbullying has many psychological effects on the victim that take time to recover from. It is the destruction of his pride, his sense of security, and a shock as a shock to his hopes and aspirations for the future. In most cases, the cause of cybercrime is a lack of awareness, vigilance and knowledge about the safe use of the Internet. In most cases, women hesitate to go to court against the offender either because of family prestige, social pressure or police abuse. This is an area where the research team really needs to work. Appropriate counselling from specialists and emotional support from family members help the victim overcome pain and anxiety. The Indian constitution has several constitutions for the benefit and protection of women. Where necessary, some special provisions were also added to ensure the rights of women. Because the government has created a cybercrime reporting platform for the prevention of cybercrimes against women and children (CCPWC). The state smart police had been tasked to keep a check on the cybersex workers by locating their IP addresses if they are found misusing the internet and committing any cybercrimes against women and children. Women in India have limited access to justice. The reason is illiteracy, social and cultural barriers, lack of support from family and subordinates, time-consuming and unhealthy legal process. This is also the main reason why most cybercrimes committed go unreported and unrecorded. A detailed analysis of all aspects must be done to solve the problem of cybercrime against women. Strict legal action should be taken against the offender. The first duty of women themselves is to get information about all the currents and to be strong and brave enough to raise their voice against such crimes. There are many unique software that detect any kind of cyber stalking and if someone is tracking an email id. So, it can be said that addressing cybercrime against women in Indian Penal Code reforms requires government policies and a change in attitude and awareness towards Indian education system and society.