International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 132-139 ISSN: 2584-2145
www.ijemh.com

Cyber Crime: Victimization of Women and It’s Legal Prevention

Sudha Malakar, *B.A.LL.B (honours), Bimal Chandra College Of Law, kalyani University. LL.M 1st year, Murshidabad University.*

Chaitali Das,*B.A.LL.B, George School of Law, Calcutta University.LL.M 1st year, Murshidabad University.*

Date of Submission: 18-03-2024 Date of Acceptance: 02-04-2024

ABSTRACT: *Social networking sites have recently gained prominence. Social networking sites are used for sharing any kind of information. In recent times, it is clear that crime against women is on the rise in all areas where cybercrime is rampant but it can be a very frustrating experience for a woman. Regarding how the digitization process is progressing, which provided the power. People are conducting study on the internet, which has made life more comfortable and convenient. They go into the unknown and engage in conversation with nearly everyone, everywhere and at any time. Cybercriminals, who mostly target women in society through various forms of crime which integrated cybercrime such as stalking, cyberbullying, harassment etc. The women are continuing to be at risk as a result of cybercrime, which has become a significant challenge for the nation’s law enforcement organizations. In India, criminals are increasingly abusing online platforms to harass and abuse women for several purposes for which they are being funded or out of revenge nature. Women are victimised day by day in the cyber word, in order for the prevention and the control of the cybercrime, there are several legal frame work which have been discussed in this paper.*

Keywords: *Social Networking Sites, Cybercrime, Crime Against Women, Digitization, Cyberbullying, Harassment, Stalking, Law Enforcement, India, Legal Framework, Prevention.*

I. INTRODUCTION

Women are highly valued in traditional Indian society. The Vedas, for example, uphold the qualities of motherhood, creation, and giving birth, and they are honoured as “Devi,” or goddesses. Because women played such a significant role, their abuse and mistreatment were seen as degrading to society as a whole as well as to the woman. In this age of technology, it is difficult to realize or imagine whether this ‘everyday changing’ aspect of technology is a blessing or a bane for us. With new software, IT-enabled gadgets, internet-enabled easy-to-use applications, technology is becoming an important part of our lives. A few years ago, the Internet could only be accessed in certain parts of the country and only on desktop computers. Within a decade the scenario has completely changed. Now the internet is accessible on a small smartphone or any handheld device The core concept of numerous technology advancements and developments is Digital India. The majority of people use computers, the internet, and other gadgets on a daily basis. The most popular devices are social media sites like Facebook, Instagram, Skype, and chat rooms, Dating apps, WhatsApp, etc. On the one hand, digitalization has improved India’s system in many areas including governance, economics, and education; on the other hand, it has resulted in a significant increase in cybercrimes in India.

However, women are now perceived as sex objects and treated differently than men in a variety of social contexts and roles. As a result, there is a strong gender bias in society and even among men, who believe that mistreating women cannot have consequences. With the blessings of Information and Communication Technology, the digital age is benefiting billions across the world. The entire world has become a global village. As the world becomes increasingly connected, cybercrime has emerged as one of the most significant threats to our society. A growing number of new crimes have evolved as a result of people using computers and the internet more frequently; these crimes are sometimes referred to as cybercrimes. Although these crimes can target any segment of society, they primarily target women group. Women are the true victims of cybercrimes in Indian society. Now pay attention to the following points that elaborate on how women are victimised by cybercrimes and provide its legal prevention.

Online shopping, web browsing and social networking are some of the major uses of internet in India. Among these three, social networking sites are a major factor that has prompted us to rethink the use of these technologies in our daily lives. Facebook, Twitter, Google+, LinkedIn, Instagram, WhatsApp, WeChat etc. Are influencing the way users maintain and develop various social relationships ranging from close friendships to casual acquaintances. These social networking sites are used for making friends, chatting, sharing pictures and videos and reading news. The use of technology in this form has given rise to the ugly side of the Internet – “cybercrime”. Cybercrime against women can be defined as any form of gender-based and sexual violence expressed through the use of the Internet and computers. Violence against women is being perpetrated

through the use of media such as email, texting, Facebook, Twitter, LinkedIn, YouTube, chatting, Instagram etc. Although these platforms were created for information sharing and communication, criminals are using them as tools. Humiliating or silencing women with shameful consequences.

UNDERSTANDING THE MEANING OF CYBER CRIME

Cyber crime comes from the terms “Cyber” means internet and “Crime” which means harmful act. Therefore the cybercrime refers to any crime that involves a computer and a network. Criminal activities that specifically target a computer or network for damage. In simple words, cybercrime refers to illegal activity committed on the internet. Cybercrime includes (but are not limited to) email espionage, software piracy, hacking, frauds, spying, phishing, stalking etc. The study here has been limited to the various types of cyber crimes against women in India.

Cyber violence uses computer technology to access women’s personal information and use the Internet to harass and exploit women. Women are becoming soft targets as they often trust other people and are unaware of the consequences. Cybercrime affects women the most by subjecting them to mental and emotional harassment. Most women feel distressed, humiliated and frustrated under such crimes which are challenging to address and resolve.

UNDERSTANDING THE CONCEPT OF CYBERCRIMES AGAINST WOMEN

Cybercrime is the term for illegal actions committed through the use of digital technologies, including computers, smartphones, and the Internet. These illegal activities can take many different forms, from fraud and theft to cyberterrorism and hacking. The primary victims of this violating act are women and children. The idea of crime, which is associated with computers and the internet, must be understood in order learn the concept of cybercrime. Cybercrime can be defined as the class of crimes that belong to the same genus as traditional crimes and that involve computers as either objects or subjects of criminal activity. Cybercrime includes all illegal activities that use computers as a tool, a target, or a way to commit crimes repeatedly.Due to the widespread use of the internet nowadays, a new category of crimes known as “cybercrimes” is growing every day. Because of the development of technology, cyber criminals now rely entirely on the internet. The internet has made it possible for cyber criminals to easily access anything while sitting still. Everything a man can imagine can be done online, including social networking, online shopping, data storage, gaming, online learning, and online employment. The use of the internet is widespread. The idea of cybercrimes emerged along with the rise of the internet and its benefits. Different ways of committing cybercrimes exist. The protection of women has always been an issue, especially in a nation like India where the rate of crime against women is rising like a coconut tree. It used to be limited to highways or remote locations. In the past, the best place for a woman to avoid being harmed was her home, but that’s not the case now. For them, home is turning into a place that is as dangerous and rife with crime. Cybercrimes are any illicit acts that involve the use of a computer as a tool, a target, or both. This phrase refers to a broad range of offenses, including phishing, credit card fraud, bank robberies, illicit downloading, child pornography, and kidnapping. Through chat rooms, phishing schemes, cyberterrorism, the production and/or dissemination of viruses, spam, and other methods. Women are most frequently the victims of cybercrime, a crime whose scope can be extended to many uncharted territories. Cybercriminals employ technology to gain access to personal information and use the internet for exploitation and abuse, including stalking, email blackmail, photo morphing, cyber pornography, etc. Today’s criminals are progressively becoming more using online platforms in India to harass and abuse women and children in order to satisfy voyeurism. The majority of victims of cyberstalking, harassment, extortion, blackmail, etc. Are women and as well as children. Women exchange their personal information with abusers or perpetrators knowingly or unknowingly frequently, which leads to a large number of cybercrimes. Many times, because the women are not aware of the process for filing a complaint, the criminals have an easier time harassing, abusing, blackmailing, etc. Them and their family. Which lead to fear against women specially for young girls. Women and as well as children need to be made much more aware of how to use smartphones, computers, and the internet safely. Therefore, it is imperative to improve women’s knowledge of the need to use caution when using internet resources and to receive correct assistance if they are ever a victim of cybercrime so they can speak out against it.

SOME MAJOR CYBERCRIME FACED BY WOMEN

Some of the major well-known cybercrimes have put thousands of women into various health issues such as depression, hypertension and women suffer from anxiety, heart disease, diabetic and thyroid ailments due to harassment. Major Cybercrimes are as under:

Cyber stalking: It is the practise of following someone with the intent to harass or harm through online. It is described as persistent, unwanted, and threatening activity that is targeted specifically at one person (the victim) and that would reasonably be expected to result in a person’s family members or oneself suffering physical harm or passing away. Cyber stalking is on the rise and women are the most likely targets. Cyberstalking is a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim but follows the victim’s online activity to gather information, make threats in different forms of verbal intimidation.

Harassment through e-mails: Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via email. E-harassments are similar to the letter harassment but creates problem quite often when posted from fake ids. The motives behind cyber stalking have been divided in to four reasons, namely, for sexual harassment for obsession for love, for revenge and hate and for ego and power trips. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites (e.g. blogs and Indy media) and email. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment.

Cyberbullying : Cyberbullying has a severe impact on women in cybercrime, leading to emotional distress, anxiety and sometimes even offline damage. Women can face reputational damage, harassment and threats online. This digital abuse can affect mental health, self-esteem and overall well-being. Addressing cyberbullying requires a multi-pronged approach, including legal measures, online platform policies and digital resilience and awareness campaigns. Creating a supportive online environment and encouraging reporting processes can contribute to combating cyberbullying against women.

Defamation: Cyber defamation includes both libel and defamation. It involves publishing defamatory information about the person on a website or circulating it among the social and friends circle of victims or organisation which is an easy method to ruin a women’s reputation by causing her grievous mental agony and pain.

E- Mail spoofing: It generally refers to an e-mail that emerges from one source but has been sent from another source. It can be causing monetary damage.

Stalking via email: It is a form of harassment that includes writing love letters under fictitious names, threatening messages, and on a daily basis sending embarrassing emails to a person’s mailbox. When one or more people send unwanted and frequently threatening electronic communications to another person on a regular basis, it is typically seen as a form of stalking. It might be difficult to define exactly what constitutes a harassing message in terms of both appearance and tone.

Phishing/online fraud : Phishing is the attempt to gain sensitive information such as username and password and intent to gain personal information. Women victims of online fraud often face challenges like identity theft, phishing scams and romance scams. Criminals can use social engineering techniques to target personal information for financial gain. Additionally, gender-based online harassment is prevalent, contributing to a hostile online environment. Empowering women through cybersecurity education, promoting safe online practices, and building a supportive digital community can help reduce these issues. Addressing the unique challenges women face in online fraud is essential for raising awareness and collaboration between law enforcement and technology platforms.

Morphing: Morphing is editing the original picture by unauthorised user or fake identity. It was identified that female's pictures are downloaded by fake users and again re-posted /uploaded on different websites by cresting fake profiles after editing it.This crime is committed with the intent to malign or exact revenge on the victim by blackmailing or defrauding them online.

Privacy violence: Privacy violence against women in cybercrime involves unauthorized intrusion into their personal space, sharing of intimate content without consent and online activities. Such violations can lead to emotional trauma, fear and compromised security. Addressing privacy violence requires strong legal frameworks, technological safeguards and awareness campaigns. Empowering women through digital literacy and promoting safe online practices can help reduce risks. Collaboration between law enforcement agencies, technology companies and advocacy groups is critical to addressing the complex challenges surrounding privacy in the digital realm.

Trolling: Trolls spreads conflict on the Internet, criminal's starts quarrelling and upsetting victim by posting disgusting or off-topic messages in an online community with the intention to provoke victims into an emotional, upsetting response. Trolls are professional abusers who, by creating and using fake ids on social media, create a cold war atmosphere in the cyber space and are not even easy to trace.

Cyber Pornography: Cyber Pornography is the other threat to the female netizens. This would include pornographic websites; pornographic magazines produced by using computers and the internet. In the name of pornographic websites, threats are made against female members of society in an effort to obtain sexual favours or get back at them. The most frequent of these charges involves editing naked photos into altered ones and uploading them to pornographic websites. Because it is so simple to access these sites, there has been an increase in major cybercrime.

VICTIMIZATION OF WOMEN IN CYBERCRIMES

Cybercrime is any illegal activity that is primarily carried out via a computer. The act of continuously, unwanted, and abusive conduct online with the intention of intimidating, demeaning, threatening, harassing, or stalking another person is known as cyberbullying. Put differently, Indian law forbids any form of harassment carried out via email, social networking sites, or chat rooms. Unfortunately, harassment and cybercrime directed towards women are widespread in modern society. These crimes can take many different forms, including online stalking, identity theft, cyberbullying, and revenge porn. One of the most common forms of online abuse directed towards women is cyberstalking. The act of harassing or following someone online is known as cyberstalking. It can take the form of sending unwelcome emails or text messages, making obscene remarks, or following someone on social media. Retaliation porn, which involves publishing a person's private or sexually explicit photos or films without their permission, is another type of online harassment. This can cause emotional and psychological trauma for the victim and be extremely detrimental to their reputation. Cybercrime and harassment of women are important problems not just in India but all throughout the world. Cyberstalking, online harassment, and revenge porn have all been prevalent forms of cybercrime and harassment against women in India.

The 2019 WhatsApp spyware assault, which targeted journalists and activists in India, including women, was one well-known instance. The attack transformed a vulnerability in WhatsApp that allowed hackers to install spyware on users' devices and access their private conversations and personal data. There have also been several cases of cyberbullying, doxing, and online shaming of women via social media platforms like Facebook, Twitter, and Instagram. To address these issues, the Indian government has created a number of laws and initiatives to shield women from harassment and cybercrime. These include the Information Technology Act, which outlaws cyberstalking, and the Cyber Crime Prevention Against Women and Children (CCPWC) initiative, which aims to provide women and children with a safer online environment. However, despite these initiatives, cybercrime and harassment of women continue to be widespread in India and around the world.

Thus, it is very clear that the victim is afraid of embarrassment and family stigma so they feel responsible for the crime. Reasons for increase in cybercrime against women According to the National Crime Record of the Government of India, 9622 cybercrime cases were registered in 2014 and 5752 them arrested. In 2015 in 11,952 cyber cases were registered which was 20% more than the reported cases of Pella and out of which about 8121 criminals were arrested and in current scenario Cybercrimes against women saw a considerable rise in 2022 compared to 2021. There has been an

11% rise in the number of cybercrimes against women in 2022. Incidents where sexually explicit material of women was published or transmitted stood at 2,251 compared to 1,896 in 2021. At the same time, other cybercrimes targeting women, such as blackmail, defamation, morphing, creating fake profiles, etc., stood at 689 in 2022 and 701 in 2021. There many women work longer hours at computers and live far away from their families. The criminal uses the internet excessively, hiding and abusing his identity. Many cybercrimes go unreported because of fear of the family and society. Indian law enforcement, however, takes cybercrime seriously. In such cases, if a woman falls victim to cybercrime, the help line or non-governmental organisation should get in touch with cyber victims' counsel so that they can assist you and direct you through the procedure.

PREVENTION AND LEGAL FRAMEWORK

Although a full regulatory framework for laws regulating the cyber domain, including such activities, has not been drafted, certain legal remedies under various statutes can assist a victims of cyber violence

The Indian Penal Code 1860: Prior to 2013, there was no law specifically addressing online abuse or crimes against women in cyberspace. Section 354A of the 2013 Criminal Amendment Act amends the Indian Penal Code, 1860 by adding Sections 354A to 354D.

Section 354A : According to Section 354A, a man who engages in any of the following acts: Demands or solicits sexual favours; Showing pornography against a woman's will; or making sexual comments-constitutes sexual harassment and shall be punished with rigorous imprisonment for a term which may extend to three years, with fine or with both. In the first two cases, imprisonment up to one year, fine or both.

Section 354C : Voyeurism is defined in Section 354C as taking a photograph of a woman engaged in a private act and/or publishing without the woman's permission. The circumstances must be such that the woman "would ordinarily expect not to be seen by the criminal or someone else acting at the direction of the criminal" to qualify as "voyeurism." On conviction under this section, the offender is liable to fine and imprisonment for a term which may extend to three years on first conviction and imprisonment for a term which may extend to seven years on subsequent convictions.

Section 354D: Addition of section 354D talks about stalking prohibition which covers online stalking. Stalking is defined as when a man follows or approaches a woman despite her apparent disinterest in the interaction, or when a man observes a woman's online behavior, Internet use, or electronic communications. On conviction of stalking, a person can be jailed for up to three years and fined, and on subsequent convictions can be jailed for up to five years and fined.

Section 503: Threats to harm a person's reputation, either to cause her panic or to compel her to modify her course of conduct about whatever she would normally do/not do, constitute criminal intimidation. The act of cyber-blackmailing a person, as was done in the aforementioned example, can be placed within the range of this law.

Section 507: This section establishes the maximum penalty for Criminal Intimidation committed by an individual whose identity is unknown to the victim. Any anonymous communication that constitutes criminal intimidation in violation of the preceding Section 503 is penalized under this section.

Section 509: In this provision any person who utters a word, makes a sound or gesture, or displays an object with the intent that such word, sound, gesture, or object is heard or seen by a female and insults or intrudes on her modesty or privacy may be charged under this section and sentenced to up to three years in prison and a fine. This section may punish cases of sexual statements or comments sent over the internet, as well as other obscene photos and content forcibly supplied through the internet.

Information Technology of India 2000

Section 66C- Identity theft is a punishable offense under Section 66C of the IT act. This clause will apply to cyber hacking. Under this provision, anyone who uses another person's electronic signature, password fraudulently or dishonestly can be jailed for up to three years and fined up to one lakh.

Section 66E : Relates to violation of a person's right to privacy. Capturing, publishing or sending images of a person's private area without their consent, or in circumstances that violate their privacy, can be jailed for up to three years and/or fined.

Section 67: Makes the publication, transmission or distribution of obscene material illegal and punishes violators with imprisonment for up to three years on first conviction and up to five years on first conviction and fine on second conviction.

Section 67A: A misdemeanour offense of facilitating publication, broadcast or transfer of sexually explicit material punishable with imprisonment for five years and fine for the first offence, and imprisonment for up to seven years and fine for the second offence.

Section 72: Punishment for breaching privacy and confidentiality diaries were all included.

CYBER CRIME PREVENTION AGAINST WOMEN AND CHILDREN SCHEME

The main objective of Cyber Crime Prevention against Women and Children (CCPWC) Scheme is to have an effective mechanism to handle cybercrimes against women and children in the country.

'Police' and 'Public' are State subject as per the Constitution of India and States are primarily responsible for prevention, detection and investigation of crime through their law enforcement machinery. The Law Enforcement Agencies take legal action as per the relevant sections of the Indian Penal Code and the Information Technology Act, 2000 against the cyber fraud offenders. The online cybercrime reporting portal www.cybercrime.gov.in has been operationalized and since inception, more than 3800 complaints have been received on it.

Following actions have been taken for effective implementation of the scheme:

Central Cybercrime Reporting Portal (www.cybercrime.gov.in) launched on 20th September 2018 to report complaints pertaining to Child Pornography (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit content. Training programmes prepared for Law Enforcement Agencies (LEAs), public prosecutors and judges. Four workshops conducted for capacity building of LEAs and officials of Ministry of Women & Child Development (WCD) under CCPWC scheme. Handbook on Cyber Safety for Adolescents/Students has been released. Cyber Dost Twitter Handle (@CyberDost) and radio campaign across the country launched for spreading awareness against cybercrimes.

RELATED INCIDENT AND CASES INVOLVING WOMEN AND CYBERCRIMES

State of Tamil Nadu vs. Suhas Katti (2004),

(C No. 4680 of 2004)

The case of State of Tamil Nadu vs. Suhas Katti (C No. 4680 of 2004) is a landmark judgment in the annals of Indian cyber law, primarily addressing the issue of cyber harassment. The case is significant for setting a legal precedent in the prosecution of cybercrimes, especially those involving defamation and harassment using digital platforms.

Facts Of the Case

In the landmark Suhas Katti case, a pivotal legal battle unfolded in the Egmore Chief Metropolitan Magistrate's court. Suhas Katti, claiming to be a family friend, faced charges for posting derogatory and defamatory online statements about Ms. Roselind, a divorced woman. His rejected marriage proposals led to a malicious campaign where he shared her number on various forums, falsely suggesting she was soliciting, resulting in numerous harassing calls to her. In retaliation for her refusal, Katti created a fake online account in her name, further tarnishing her reputation.

The victim's February 2004 complaint under sections 67 of the IT Act, 2000 and sections 469 and 509 of the IPC, led to Katti's arrest. The charges included forgery for harming reputation (IPC 469), intending to insult a woman's modesty (IPC 509) and publishing defamatory content electronically (IT Act, Section 67).

Case Issues

In State of Tamil Nadu vs Suhas Katti, a fake account was set up in the name of Ms. Roselind with the intention to harm her reputation, facilitating the spread of derogatory statements through Yahoo groups.

In response to these actions, a complaint was lodged in February 2004 under Section 67 of the Information Technology Act, 2000 and Sections 469 and 509 of the Indian Penal Code, 1860. The police apprehended the accused, a friend of the victim residing in Mumbai, subsequent to the complaint.

Judgment

On November 5, 2004, Additional Chief Metropolitan Magistrate issued the following ruling: "The accused is found guilty for the offence committed by him, and for which he must be found guilty and sentenced to undergo rigorous imprisonment for 2 years, a fine of Rs. 500/- under Section 469 of Indian Penal Code, and for the offence under Section 509 of Indian Penal Code, the accused is sentenced for 1 year." And pursuant to Section 67 of the Information Technology Act of 2000, the offender faces a harsh 2-year jail sentence and a fine of Rs. 4000.The accused must pay the fee and serve their time in central jail in Chennai.

Ritu Kohli case:

Ritu Kohli Case was India's first case of cyber stalking, in this case Mrs. Ritu Kohli complained to police against a person, who was using her identity to chat over the Internet at the website http://www.micro.com/, mostly in Delhi channel for four consecutive days. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu Kohli at add hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on add hours. The said call created a havoc in personal life of the complainant consequently IP addresses was traced and police investigated the entire matter and ultimately arrested the offender. A case was registered under the section 509, of IPC and thereafter he was released on bail.

This is first time when a case of cyber stalking was reported Similar to the case of email harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the IT Act that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women.

Rashmika Mandanna Case, Delhi:

In a more recent instance, famous actress Rashmika Mandanna was the victim of cybercrime as well. She was the victim of illegal morphing through Artificial Intelligences and circulates its through internet. The Delhi Police on Friday registered a First Information Report (FIR) at the Special Cell police station in connection with deepfake AI-generated video of actor Rashmika Mandanna, the police said. The Delhi Police have registered the FIR under relevant sections, and an investigation has been carried out into the matter.

"In regard to the deep fake AI-generated video of Rashmika Mandanna, an FIR u/s 465 and 469 of the IPC, 1860 and section 66C and 66E of the IT Act, 2000 has been registered at PS Special Cell, Delhi Police and an investigation has been taken up," the Delhi Police said.

II. SUGGESTIONS

- The laws that currently exist in our nation are adequate to provide victims of this kind of harassment with justice because they include penalties; however, as technology advances and artificial intelligence grows at a rapid rate, might be an instrument for harassing women online, a practice for which appropriate regulation is needed.
- Spread awareness of cybercrimes and female harassment by utilising public awareness campaigns, social media, and other channels. This might encourage victims to come forward and seek assistance, helping to create a society that disapproves of such behaviour.
- Women should be taught about internet safety. Education regarding online safety and self-defence against cybercrime and harassment is crucial for women.
- For this, public awareness campaigns, online courses, and workshops can all be helpful.
- Women are soft hearted and emotional, under trust and believe they knowingly or unknowingly invited more vulnerable cybercrime for which their life became measurable. Women should control their emotion and put three Words in their minds i.e., Why, How and What.
- Simply block people you don't want too intact you.
- Always use strong passwords and don't share passwords; it may sound pointless.
- Reporting a cybercrime: This is very important that every woman must report any such cybercrime without any hesitation.
- Spread awareness: It is imperative to increase awareness regarding the problem of cybercrime and harassment directed towards women. Campaigns on social media, open gatherings, and other awareness-raising techniques can help achieve this.
- Be alert for fake or irrelevant phone or email messages.
- Avoid responding to emails that ask for personal details.
- Be careful when visiting fraudulent websites that aim to steal your personal data.
- Cybercrime jurisdiction can be a problem, as there is a lot of unciea or absurd information regarding The jurisdiction to file a complaint, when you women or women from rural areas face problems online or they are raped by fraudsters, they do not know where to file a complaint . Complaints for this the government should take appropriate measures and spread awareness through online campaigns or offline programs or online courses to address these issues.

III. CONCLUSIONS

There is no denying that the impact of the increase in internet usage has been both positive and negative. On one hand it has helped individuals in better decision making, better livelihood, entertainment, easy and affordable education, development of e-commerce etc. And on the other hand it has given rise to crime in the virtual world.

The relationship between internet users and cybercrime cases is significant. The use of internet is increasing all over the world, so the occurrence of cybercrime is inevitable. Women tend to be soft-hearted, under stress and trust others with property easily – making them more vulnerable to cybercrime. The need of the hour is that by adopting various preventive measures we can reduce the increasing incidence of cyber crimes against women. Although there are strict laws against cyber crime, there is a problem in implementing these laws due to some reason. As they deal with issues like online bullying and identity theft more than men, we need to take action to make things better. In an increasingly technology-dependent world, cyber violence is on the rise, with women becoming soft targets. The law must go the extra mile to punish such criminals with strict action.Prevention of cybercrime against women requires greater awareness and knowledge about cyber practices, privacy protection and legal security. Thus awareness of increasing privacy settings on social networking sites as a preventive measure. So, there is an urgent need to bring awareness and awareness among women to take precautions while using internet facilities and also a proper guidance so that if they face cybercrime in any way they can raise their voice against it. There is also a pressing need for knowledge and technological improvements to prevent harassment of women in India.

REFERENCES

[1]. Cyber obscenity and victimisation of women in India. (2017, May 9). Retrieved from i pleader : https://blog.ipleaders.in/cyber-obscenity/#:~:text=Online%20gender%20harassment&text=Cyber%20spaces%20have%20become%20havens,also%20the%20victims%20of%20cybercrimes

[2]. Gaur , kd(2019) Indian Penal Code,(Eighth Edition) Universal LexisNexis

[3]. LawBhoomi. (2024, January 29). Law Bhoomi. Retrieved from https://lawbhoomi.com/state-of-tamil-nadu-vs-suhas-katti/#:~:text=Suhas%20Katti%20(C%20No.,and%20harassment%20using%20digital%20platforms

[4]. Ministry Of Home Affairs . (2021, January 18). Retrieved from https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme

[5]. Mishra, S. (2018). Dimensions of Cybercrime Against Women in India – An Over View . International Journal of Research And Analytical Review , volume 5 .

[6]. N.D. (2023, November 11). Delhi Police Files Case Over Actor Rashmika Mandanna,s Deefake Video. Retrieved from NDTV: https://www.ndtv.com/india-news/delhi-police-files-fir-in-deepfake-video-case-of-actress-rashmika-mandanna-4565845

[7]. Rajkumar, A. (2023, december 5). The News Miniute . Retrieved from https://www.thenewsminute.com/news/crimes-against-women-rise-by-4-cyber-crimes-increase-by-11-ncrb-data

[8]. Sharma, D. (n.d.). Cyber crime In India : Are Women A Soft Terget . Retrieved from Legal Service India E Journal : https://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target.html

[9]. Shyampada Ghorai, D. N. (n.d.). Study on the case laws Registerded regarding Cyber crime Against Women . Journal of Advances and Scholarly Researches in Allied Education | Multidisciplinary Academic Research.

[10]. SURAKSHAP. (2022, DECEMBER 7). THE ECONOMIC TIMES. Retrieved from https://m.economictimes.com/tech/technology/only-2000-odd-people-arrested-in-more-than-10000-cybercrime-complaints-in-2021/articleshow/96058866.cms