CYBERCRIME AGAINST WOMEN IN INDIA: IDENTIFICATION AND MITIGATION

Tanu Kapoor, Rajiv Gandhi National University of Law, Patiala, Punjab

ABSTRACT

Cyberviolence against women is a growing global issue that may have significant social and economic repercussions. This is a result of the rise of social media, the proliferation of mobile devices, and the expansion of the internet. Cyber violence refers to any form of sexual or gender-based violence against women that occurs via ICTs such as the Internet, mobile devices, and video games. These technologies are ideal for use as weapons against women for a variety of reasons, including cyber stalking, sexual abuse (including sending the victim sexually explicit or pornographic emails), cyber extortion, cyber bullying, cybersex trafficking, and phishing. Even if there are more crimes against women in general, a cybercrime can be the most distressing thing that has ever happened to a woman. Even more so in India, where women are devalued and cybercrimes receive little legal consideration. It is demonstrated that Cyber Crimes against Women are not adequately addressed by the current rules and practises of India's legal system. In addition, we must consider a number of solutions for the increasing frequency of cybercrimes against women in India. At the conclusion, we discuss the options available to victims of cybercrime and the modifications that should be made to the overall legal framework to combat the rising tide of cyber crimes.

Keywords: Cyber Crime, Women, Violations, Laws, Covid, and Challenges.

1. Introduction

The options for privacy that women have in cyberspace are more limited than those that men have. More and more people are using computers and mobile devices to access the web and share data. Our work, communications, and social interactions have all been significantly impacted by the rise of cyberspace and the way consumers now access information and form connections. Transferring anything into cyberspace automatically exposes it to a wide variety of cybercrime. As the popularity of social networking sites continues to rise, new forms of cybercrime, such as those involving these sites, are emerging to take advantage of the vast amounts of personal information that people share online. The law protects individuals from cyberstalking, cyberbullying, e-mail spoofing, morphing, and defamation. Knowing the user has been hurt online has real-world repercussions. Due to the widespread availability of information technology, this problem has been made worse by a lack of knowledge in specific areas. A future study will look at cybercrime anxiety across industries and try to pin down the role that training and education play in alleviating people's concerns about cyber threats.

While it may be impossible to completely eradicate crime, we can take steps to make our communities safer. Policymakers and law enforcement agencies in a technologically advanced society must take measures to deter cybercriminals. There are benefits and drawbacks to technological advancements. Many statutes address cybercrime directed at women. Lawmakers and government officials have a responsibility to ensure that technological advancements are not only possible, but also moral. Criminal activity rises in tandem with the rise in internet usage, particularly among vulnerable populations like women. The number of incidents of cybercrime against women in India is on the rise. Young people commit adultery, flirt, and even start virtual fires. Women in India have good reason to be concerned about negative portrayals of them in the media.

When women spend more time online without being aware of the dangers, they put themselves at risk. It is unacceptable to harass women online. At the same time that cybercrime is growing, so too is the field of cyberlaw. These cyber-threats necessitate legal responses. Quickly alerting governments and cyber law organisations is essential. India sponsored studies of internet behaviour in 2013 and 2014. In 2014, India hosted a conference on cyberlaw. International and scholarly cooperation were both boosted by these initiatives. While there is a lack of cyber courts in India, the country's police force is among the best-trained in the world. Online crime

has not decreased.

2. Literature review

The Ritu Kohli case was the first instance of a cybersexual offence being reported in India. Manish Kathuria was arrested by the Delhi Police's crime branch for using the profile of an Indian woman, Ms. Ritu Kohli, to engage in illicit online chat. He invited random people to call her at home, using obscene language, and he even gave out her phone number. As a result, Ritu kept getting harassing calls from people all over the world. Unexpectedly, she went to the Delhi police with her story. The police moved quickly, identified the offender, and charged him with violating Ritu Kohli's modesty under sections 67 of the Information Technology Act and 509 of the Indian Penal Code.

The first case in India to result in a conviction for cyberpornography was Suhas Katti v. State of Tamil Nadu in 2004. Katti was given the following sentences for his transgressions: two years of rigorous imprisonment and a fine of 500 rupees for violation of section 469 of the Indian Penal Code; one year of simple imprisonment for violation of section 509 of the Indian Penal Code; and two years of rigorous imprisonment and a fine of 4,000 rupees for violation of section 67 of the Information Technology Act, 2000. (Criminal penalties for sharing pornographic material online)

The case of the student at Air Force Balbharati School (Delhi) who was teased for having a pockmarked face in 2013 is an example of this. He got the bright idea of scanning photos of his classmates and teachers, morphing them with nude photos, and posting the results to a website hosted by a free web hosting service as a means of getting even with his tormentors. The parent of one of the girls depicted on the website reported this to authorities. Sections 43 and 66 of the Information Technology Act of 2000 make this kind of behaviour illegal. The perpetrator could also face charges under Section 509 of the IPC.

An employee (the defendant) of a company started sending insulting, defamatory, and obscene emails about the managing director of the company in SMC Pneumatics (India) Pvt. Ltd. v. JogeshKwatra-Jogesh Kwatra, the first case in India to report cyber defamation. Attempts were made, via anonymous and frequent emails, to damage the plaintiff's good name and reputation with its business partners. With the help of a private computer expert, the plaintiff was able to pinpoint the defendant and file a complaint with the Delhi High Court. An injunction was

issued by the court barring the employee from sending any more emails that are defamatory or otherwise harmful to the plaintiffs.

To defraud and blackmail an NRI living in Abu Dhabi, the most well-known case of cyber spoofing is Gujarat Ambuja's Executive Case (1998) AIR 2000 MP 194, 2000 (2) MPHT 112.

A woman was found guilty of cyberstalking for the first time in Maharashtra in the case Yogesh Prabhu v. State of Maharashtra, which was decided in July 2015 by the additional chief metropolitan magistrate M.R. Natu. Prabhu's conviction comes under both Section 509 of the Indian Penal Code and Section 66E of the Information Technology Act of 2008. (Consequences for invasion of privacy)

Imtiaz Ahmed v. Durdana Zamir (2009 SCC online Del 477: (2009) 109 DRJ 357: 2009 INDLAW Del 119), a case involving defamation, was decided by the Delhi High Court. A statement is considered defamatory if it causes reasonable people to think poorly of the plaintiff. A claim is assessed in light of the norms of reasonable people living in the time period in question. The words must have conveyed an accusation against the plaintiff or denigrated his office, profession, calling, trade, or business; caused him to be avoided or shunned; caused him to be viewed with hatred, contempt, ridicule, fear, dislike, or disrespect; or caused him to feel disrespected. The defendant must pay monetary damages to the plaintiff in such a case. Courts have the authority to award compensation to victims of defamation when someone else's good name has been sullied through reckless or reckless behaviour. In India, the tort law has not been updated.

The DPS MMS scandal is a prime example of this phenomenon because it involved the creation and widespread distribution of an MMS clip of a schoolgirl engaging in sexually explicit behaviour. Separately, a Swiss couple forced children from Mumbai's slums to pose for pornographic photographs that were later posted on paedophile websites. The Mumbai police arrested the couples on charges of pornography. The recent case of the leak of CCTV footage from the Delhi Metro, in which images of couples engaging in intimate behaviour in metro stations, etc., were captured by police security cameras, is a good illustration of this phenomenon.

3. Statement of problem

Society, government, families, and individuals must act swiftly in response to cybercrime. There are few reliable crime statistics available, and the majority of crimes go unreported. Prevalence and prevention of cybercrime require specific and effective research. Since 1995, Internet usage has skyrocketed. Later, scholars investigated similar issues. This study examines methods for protecting women and girls from cybercrimes and preventing their occurrence.

4. Research objectives

i. To learn more about how cybercriminals target women.

ii. Determine the most effective means of preventing women from becoming victims of cybercrime.

iii. To shed light on legal arrangements regarding cybercrime against women.

5. Methodology

This article was written considering the doctrinal or non-empirical research methods. This article will employ critical thinking and investigation to examine current dispute resolution protocols and case law. Using essential and supplementary sources, such as the law, case law, legal course readings, critiques, books and websites on the internet, news articles, and other unfamiliar publications and periodicals, among others, this paper attempted to validate all assumptions. The ebb and flow Study makes use of both analytical research and ex post facto (done, created, or determined after the fact).

6. Discussion and result

Cyberspace, the virtual world created by computers, is regulated by cyber laws. These rules apply to users everywhere in the world. Cyber law regulates the operation of computer and network systems. Testing for a global pandemic. There was a lack of access to medical care, people suffered from lockdowns, job losses, and the deaths of loved ones. Millions of people have lost their lives due to the COVID-19 epidemic. Millions of people's lives have been devastated by the pandemic; this includes those who have lost their jobs or had to close their businesses due to lockdowns, as well as those who have lost a loved one. Incorrect! In the midst

of the pandemic, cybercrime and mobile criminality both exploded in popularity. Some people used the internet and mobile devices to torture others during the pandemic. As a result of the pandemic, cybercrime increased dramatically.

7. Cybercrime

Cybercrime is not even mentioned in India's IT Act of 2000. The Indian Penal Code, which dates back to 1860, is the primary legal document outlining criminal offences and their associated punishments. Cybercrime is the intersection of criminality and technology. There is a broad spectrum of illegal activities that can be classified as cybercrime. A cybercriminal can commit an offence against another online without ever meeting the victim in person or revealing his or her true identity. In cybercrime, computers and data are both the target and the tool. All of these actions constitute cybercrime.

The Internet and other technological advancements are undermining the rule of law. Conventional law enforcement methods are ineffective against online crime because of the global nature of the Internet, the absence of regulation, and the accessibility of criminals. The criminal law as it currently stands is insufficient in light of contemporary criminal strategies and communication tools. It's hard to detect, report, and prove that cybercrime has occurred in India. Due to the need for the assistance of computer experts, computer crime is neither audited nor policed. Legal professionals struggle to make sense of cybercrime, e-commerce, digital signatures, and online transactions. Considering how far society has progressed toward modernity and decriminalisation, antiquated legal codes have become largely obsolete. The current state of affairs is precarious. Having physical proof is crucial. Since the internet has wreaked havoc on the judicial system, cybercriminals have adapted their techniques to account for this new reality.

The Information Technology Act of 2000 (Kumar, A., and Ranjan, A. P., 2022) does not protect women's rights, despite the fact that the Indian constitution guarantees women the same rights as men in areas such as life, education, health care, nutrition, and employment. The Information Technology Act of 2000 does not include a provision prohibiting violence against women, in contrast to the CCP, the Constitution, and the Indian Penal Code. An elite group has been convened by the government to assess the current state of cybercrime and suggest solutions. Following the meeting, the public authority assumed management of CCPWC to implement the recommendations made. Penalties provided for under the IT Act

shall not relieve the offender from liability under any other law, and the Indian Penal Code shall continue to apply in all cases, as stated in Section 77 of the IT Act. Invasions of privacy, cyberstalking, and other forms of digital harassment and intimidation occur frequently.

8. Reasons behind victimization of females:

i. **Sexual Orientation and Gender Roles:** Women's senses of their own femininity are harmed. To shield themselves from online abuse, many women who blog or comment use pseudonyms of the opposite gender. Those who identify as women but are subjected to online harassment may feel pressured to "cover," or act in more traditionally masculine ways. In order to deter cyberattacks, women downplay traditionally feminine traits like compassion and upplay traditionally masculine traits like aggression. For women, experiencing sexual harassment online can be a barrier to moving up the corporate ladder. Possible immediate effects on women's employment include cyber attacks on feminist websites and employer reluctance to hire women. Attempting to undermine women's success in their chosen fields may be a covert strategy for undermining those individuals' own careers.

ii. **Social Concerns About Defamation:** Women's reluctance, shyness, and fear of smearing the family's reputation lead them to not report most cybercrimes. She tends to hold herself responsible for the wrongs done to her. Cybercriminals target women more often because they can't be sure of the true identity of the person threatening or blackmailing them online. As a result of these concerns, many victims of crime are female, which boosts the confidence of those who commit them.

iii. **The Cyber-Attacks Against Women Problem Is Not Being Addressed by Existing International or Domestic Laws:** After initial passage in 2006, the Information, Communication, and Technology (ICT) Act was revised in 2013 to fully implement the National and Communication Technology Policy of 2002. In 2002, the policy was put into place to bring attention to the need for legislation to safeguard against cybercrime, ensure data security, and safeguard the freedom of information. Although the Act was passed in an effort to safeguard cybercrime victims, it does not cover every facet of the issue. Online and mobile phone-based harassment of women is a common problem today. There is currently no comprehensive law that adequately addresses sexual harassment in social media and other digital platforms, though cases can be filed under the Women and

Children Repression Prevention Act of 2000, the Information and Communications Technology (ICT) Act of 2006, the Pornography Control Act of 2012, and any other ordinary laws. Inadequate machinery and inadequate legislative implementation are the main issues.

iv. **More and more people are using MPSNS to make and maintain connections with others.:** Due to their widespread use and widespread popularity, social media platforms like Facebook and Twitter, as well as Google's own Google+ and YouTube, have become indispensable to modern society. A number of different multitasking platforms are available through MPSNSs, as was previously stated. Most people on Facebook use it to make new friends and connect in other ways. The resulting connections might defy the norms that confine the human mind. When people on the MPSNS learn about tragedies a user has experienced, no matter how small, they may feel compelled to offer their support and encourage the user to take the steps they believe are necessary.

v. **Insufficient Female Education:** One of the main causes of the increase in sexual crimes on MMNS is the users' lack of awareness, especially women's, that they are vulnerable targets (MPSNSs). As was previously stated, most sexual assaults happen when the victim gives the offender access to her personal information or communication. Many victims of cyberbullying continue to communicate with their aggressors even after being warned repeatedly to delete any trace of their relationship with the offender. Furthermore, many female victims and parents of minor victims immediately attempted to contact the hackers to have the offensive posts removed, or they wrote back to the perpetrator and threatened him with dire consequences. This irrational response only encourages the harasser to continue their aggressive behaviour, which compounds the victim's distress.

vi. **Patriarchal society and discrimination:** The pervasiveness of patriarchy and prejudice is often cited as the primary cause of women's subordination. In Indian culture, this system has been in place since mediaeval times. It was generally accepted that a woman's role in society entailed nothing more than taking care of the home and its inhabitants, raising children, tending to their health, and caring for the elderly. They were not allowed to have a voice in official proceedings or engage in religious, cultural, social, or political activities. Women were obligated to follow the rules and guidelines set forth by the men. The majority of the world lives in a patriarchal society that discriminates against female

children and favours male children. Girls and women are deprived of food, healthcare, an education, and economic opportunities as a result of sexism and prejudice. They are unable to update their knowledge, abilities, and tools to reflect the current era.

vii. **Inappropriate Behavior on the Part of Law Enforcement and Officials:** The following are some of the most common reasons why police will not open an investigation:

1. There is no proof that the harasser was referring to the victim when he used her name in his defamatory writings. The harasser has used his First Amendment rights to express himself. The police cannot suppress free speech without solid evidence.

2. In addition, there is no age requirement for joining cyber communities like Facebook, Orkut, Myspace, or Instagram; many users are unaware of basic security measures like filtering emails, locking personal albums and information, personal walls of social networking sites, sharing personal details and emotions with virtual friends, chat room patterns, etc.

viii. **Those who are victims of online fraud:** As the most defenceless members of society, women were prime targets for cybercriminals during the epidemic. During the pandemic, people who used social media and stay-at-home mothers were particularly vulnerable. The National Commission on Women predicts that by 2021, cybercrime against women will rise during a lockdown and then fall after the situation is stabilised. There was a dramatic increase in cybercrime committed against women in April and May of 2021 as a direct result of the second wave of attacks launched by Covid-19. There was a noticeable drop in cyberattacks beginning in June, which persisted through the month of July as the second pandemic wave passed and lockdown restrictions were relaxed. Prior to the virus's outbreak and subsequent shutdown, cybercrime against women was unusual.

ix. **Abusive content directed at females on the internet:** Despite the lockdown and epidemic, many people continued to use the internet for academic, professional, and social reasons. Laptops, smartphones, and the internet have made it possible for women to work from home. It is mandatory for female students to engage in online coursework and extracurriculars. Increases in cybercrime occurred as more women began using the

internet for work, school, and fun. The trauma of being locked out extended beyond physical harm to the victim's mental health. Some of the most common forms of online violence against women include the following:

1. Different forms of cyberstalking exist, such as making unwanted phone calls or texting the victim, or posting threatening comments on the victim's Facebook page. This scholarly tome on the life and work of B. D. Sharma was released in 2021. A survey found that 62.5% of online harassment occurred in electronic communication settings like email and chat rooms. New victim protection laws were written with Ritu Kohl in mind. By using electronic communication services to distribute pornographic material, you could face up to three years in prison and a fine under Section 66A of the ITAA 2008.

2. It is common knowledge that women account for the epidemic's lion's share of this crime type. Thieves use blackmail to coerce victims into handing over private photographs or digitally altered images in exchange for sexual favours or financial compensation. Frustrated criminals used letters and video conferences to threaten women with sex in an effort to keep women in their control during the pandemic. Despite their lack of funds, they were able to threaten others by posting fake photos online.

3. Online hacking incidents were front-page news during the pandemic. The prevalence of disinformation and hoaxes is growing. Their sensitive information was gathered, their microphone and camera were activated, and private photos and videos were taken after they clicked on a malicious URL. Criminals commit sexual and other types of crimes using the data and images.

4. Negative comments are posted on the victim's page and the cyberbully may ask for money to have them deleted. More than that, the victim's private or altered images are traded in secret, often without her knowledge or permission (Singh, J. 2015). To harass or abuse someone online, you can use any electronic device you like: computer, mobile phone, or laptop.

5. There are many other ways to misuse computers, phones, and the internet besides phishing. A victim's device is infected with malicious software after they fall for a

phishing email's lure and click on a link in the message. With regards to idioms (Jagdish Singh 2015). By using the victim's ledger and other identifying information, the criminals commit identity theft and fraud.

6. People's photos have been used for pornographic purposes by online predators. As of December 31, 2015, 857 pornographic websites had been shut down due to moral concerns. The ban was lifted by Ravi Shankar Prasad. Since one's sexual orientation is a matter of personal choice, the government has no business dictating moral standards for its citizens. Access to pornographic websites or foreign ISPs is not restricted. Singh claims that the definition of "child pornography" is undefined by law, despite the fact that it is illegal (2015). Sexual activity within the home needs to be decriminalised. To put it bluntly, the IT Act places no limits whatsoever on pornographic material that can be accessed via the Internet. Put it away on your desktop, phone, or other convenient storage device. The courts in India have ruled that pornographic content on the web is essential to maintaining "public order." "Legal maintenance" is what Kumar A. and Ranjan A. call it in their article of the same name. What follows are discussions of cyberpornography: A.E. 66, 67, 67A, and 67B. Except for sections 67A and 67B, the pornographic bail provision in Section 77B of the Information Technology Act of 2000 is legal.

7. Victims of cyber trafficking rarely, if ever, get to know their abusers face to face. Cybersex trafficking involves the public broadcast, recording, or photography of a victim's sexual or intimate behaviour, followed by the sale of this content online. Women were the target of cyberstalkers' intimidation and threats.

9. Patterns identification for cyber crimes:

i. **The Creation of a Female Avatar:** Harassers who use fake avatars to target and assault women are more successful when using MPSNSs. In order to maliciously harm the victim's reputation and mislead viewers about the victim's true identity, the perpetrator may use digital technology to create a false representation of the victim, with or without the victim's visual images, and carrying verbal information about the victim that may or may not be completely accurate.

ii. **The Transmission of Sexual Messages:** One of the most common ways women are

sexually victimised on MMNS is through the use of a fake avatar, and another is through the sending of explicit messages (MPSNSs). This can be done in three ways: (a) communicating on MPSNSs; (b) bullying; and (c) grooming women for sexual crime. The victim may be the target of sexually abusive comments made on public message boards accessible to the entire group.

iii. **Sexist and Sexual Violence Against Women Availability via the World Wide Web:** Friends and close contacts can tag a user in a location, photo, or status update on social networking sites like Facebook, Twitter, and others, giving non-friends of the user access to the user's information. Similarly, a user's Twitter followers can be limited to only those they choose to follow them if they so choose to keep their profile private. Neither Facebook nor Twitter prevents others from accessing and viewing the primary information if the user has made that information public. Under these circumstances, the person using cyber support is open to both offline and online forms of harassment and abuse.

iv. **Stalking via the Internet:** This has been one of the most widely reported instances of cybercrime recently. Tracking someone's online activities can be accomplished in a number of ways, including posting on message boards and chat rooms they frequent and sending them numerous emails. Women who are the targets of unwanted romantic advances from men are disproportionately likely to experience cyberstalking. Cyberstalkers can find and harass their victims through a variety of online mediums, including websites, chat rooms, discussion forums, open publishing websites, and email. Sexual harassment, love obsession, vengeance, hatred, and ego and power trips are all possible causes of stalking behaviour.

v. **Insults on the Web:** Also common is cyber tort, which includes defamation and slander, directed at women. This is the case when online or computer-based defamation takes place. Pneumatics (India) Private Limited by SMC Just keep saying "Jogesh Kwatra" Cyber defamation was reported after a company employee (defendant) sent offensive and defamatory emails about the company's Managing Director. Anonymous and frequent e-mails were sent to numerous business associates of the plaintiff company in an effort to damage its reputation and goodwill. The plaintiff hired a private computer expert to help them find the defendant and file a lawsuit in the Delhi High Court. A preliminary

injunction was issued by the court.

vi. **Morphing:** Morphing is the process of altering an image in such a way that it no longer resembles the original in any significant way. In order to make it seem as though young women from social networking sites like Facebook are engaging in sexually suggestive behaviour, cybercriminals frequently download their images and superimpose them on those of another woman. The next step is usually an attempt at blackmailing the women by threatening to reveal the morphed images and bring down their social standing.

vii. **Copied Emails:** E-mail spoofing refers to the fraudulent practise of sending emails that appear to have come from a different sender by forging the email's From, Return-Path, and Reply-To headers. Cybercriminals frequently employ this strategy to acquire sensitive information and private images from unsuspecting women, which they then use to blackmail the victims.

viii. **Internet blackmail:** One form of cybercrime involves the use of blackmail in which the victim is threatened with having her personal information made public, being falsely accused of wrongdoing, having her reputation damaged, etc., if she does not comply.

ix. **Hateful Disinformation on the Internet:** A message sent to multiple people with the intent of inciting hatred against the recipient because of his or her religion, race, gender, sexual orientation, or other trait. Additional forms of cybercrime that target women include cyber-grooming, cyber-bullying, forced pornography, obscenity, and offensive communication.

10. Mitigation tools and guidelines for corrective measures to prevent cybercrime:

Detection techniques are used to locate potential threats. Common network scanning tools like Nmap are first on their list. The tool is distinguished by its utilisation of TCP/IP fingerprinting for the purpose of determining the operating system. As a host-based scanner, Nessus looks for security flaws on a single host. This vulnerability scanner has an exceptional user interface. You can add Retina to the list of great scanners. Many different kinds of equipment are used in real-world investigations. For example, Nmap, Nessus, and a scan would be used to check a web server for security flaws.

There are protective technologies in place because dangers were discovered using detection

tools. They amplify the inclusion of host- and network-based defences in the threat assessment. When it comes to protecting a network, routers often serve as the first line of defence because of their crucial role in directing data to its proper node. Firewalls act as the second line of defence in a safe network, limiting exposure to danger by screening incoming data and letting in only authorised traffic. Signature-based IDSs act as network burglar alarms by identifying malicious traffic. Intrusion detection systems such as Snort are a great illustration. They lessen danger by raising people's consciousness about the issue.

Risk is evaluated using analytical approaches. What occurred, how it occurred, and the results are all factors in their assessments. Analytical software includes the NIX-based Coroners toolkit and the Windows-based EnCase. It is impossible to overstate the significance of having solid technical skills when using these toolkits. In order to be employed in the field of cyber-forensics, one must meet a number of criteria. A few examples of these traits are the ability to use redundant data sources, a high ethical standard, a commitment to lifelong learning, and an understanding of the technical consequences of one's actions.

11. Legal provisions

Despite the lack of a formal regulatory framework, numerous statutes exist to protect victims of cyber-assault. Abuse and harassment of women on the internet were not illegal until 2013. The 1860 Penal Code did not have such a provision. Changes were made to the Indian Penal Code in accordance with Section 354A of the Criminal Amendment Act of 2013. A man can face up to three years in prison, a $2,500 fine, or both for engaging in sexual solicitation or requesting a woman's sexual services, displaying pornography without her consent, or making sexual comments. Without the woman's permission, voyeurism is a crime. A victim of voyeurism "must have reasonable expectation that she will not be observed by the offender or anyone acting at his direction," according to the law. Those convicted for the first time face a three-year prison term, while those convicted multiple times face seven. The act of cyberstalking is now considered a crime thanks to 354D. Cyberstalking occurs when a man follows or watches a woman who is not interested in him online. First-time offenders face a maximum of three years in prison plus a fine, while repeat offenders face a maximum of five years. Cybercriminals may face punishments under other laws in addition to those included in the amended Code. Include:

1. Slander is defined as an attack on a person's character or reputation, as set forth in Section

499. When defamatory statements are published, the author faces up to two years in prison, a fine, or both. When someone's good name is on the line, Section 503 forbids it (Sharma, B. D. 2021). Indicatedly, cyberextortion falls under the purview of this law.

Potentially severe consequences for (Sharma, B. D. 2021) Threats made by an unknown offender are defined as criminal intimidation in Section 503. Violators of this section face the same penalties as those for Section 503 violations plus additional sanctions.The maximum penalty is three years in prison and a fine for making, using, or displaying anything that degrades or invades a woman's private space. Inappropriate sexual comments, images, and content are prohibited by this clause.

2. Information Technology Act of 2000: A violation of Section 66C of the Information Technology Act constitutes a criminal offence. This predicament pertains to hacking. This law provides for up to three years in prison and a fine of Rs. 1 lakh for the unauthorised use of another person's electronic mark, secret key, or other unique identifying characteristic. Section 66E of the Privacy Act governs the disclosure of personal information due to a security breach. Without the subject's consent, taking a photograph of a private part of their body can result in a fine and/or jail time of up to three years.

3. In Section 67, profane substances are banned, and offenders face up to three years in prison and a fine for a first offence, and up to five years in prison and a fine for a second offence.

It is a primary offence punishable by up to five years in prison and a fine under Section 67A of the Civil Code to distribute a physically identifiable substance that is also the subject of a crime punishable by up to seven years in prison.

Title IX of the Civil Rights Act of 2012, Prohibiting Sexual Orientation and Gender Identity in Mass Media. The law outlaws demeaning or sexually suggestive images of women in print, broadcast, and online media. To protect women from demeaning portrayals on the Internet, laws must be updated to cover online media (Sharma, B. D. 2021). The law was nullified when it ran out of time in 2021.

12. Some Suggestions and Steps to Tackle Cyber Crimes

There is a risk of women becoming their own cyber victims, and this trend needs to be recognised and fought against. Cybercrime laws vary widely from country to country.

Nowadays women want to feel safe and protected while they are online. There needs to be a response. Women can protect their privacy in cyberspace by following these guidelines.

In order to maintain the confidentiality of any information stored online, it is imperative that passwords be changed regularly (Pennell 2012). Passwords are used to protect sensitive information on phones, emails, landlines, banks, and credit cards. Don't let on too soon about your plans (Moore, 2009). Passwords can be made secure by using any combination of letters, numbers, and special characters. Passwords should not be simple words from a dictionary, dates, or information related to the site itself (Online Privacy & Safety Tips 2010). Protecting personal information with passwords is common practise.

To maintain your status as a successful entrepreneur, it's best not to give out your personal address. Having a job or a mailbox will do. Defending children from predators on the internet (Moore 2009). Women especially should not share private information online.

Issues like stalking, financial dishonesty, libelous behaviour, inappropriate use of email and social networking sites, virtual rape, cyber pornography, email spoofing, etc., should be given more attention in educational institutions (Halder and Jaishankar 2010). Current anti-cybercrime initiatives are being implemented.

Investigate adult internet usage with help from government agencies, social service organisations, and philanthropies. Singh argues that authorities and NGOs need to be educated about cybercrime (2015). Second, in order for police to properly investigate and understand victimisation allegations, they must undergo specific training. Participants from the academic community, the legal profession, and the non-profit sector must regularly attend seminars and workshops (Halder and Jaishankar 2010: 22).

Indian women need protection from cybercrime. To combat cybercrime, India needs either a new cybercrime statute or an amendment to the country's Information Technology Act (Halder and Jaishankar 2010: 22). We can make the world a better place if we just enforce the law.

We reserve the right to track your text messages and listen in on your phone calls. Contact the police if the harasser calls again (Halder and Jaishankar 2010: 21). Buy only from reputable software vendors. They need to be honest about what they're doing online with their parents, partners, or spouses. You can control how various online services treat your personal

information by adjusting their settings. One must be familiar with and abide by all relevant privacy policies. Learn how to adjust your social media account's privacy settings (Pennelli 2012).

Fight According to the research of Singh, J., cyberstalkers frequently use malware such as worms, Trojan horses, and email infections (2015). Antivirus software must be regularly updated to protect against Trojan, email, and worm infections (Pennelli 2012). The trend of cyberbullying can be stopped.

Keep an eye out for any untoward activity involving your account on the network. Check your inbox, blog, and online profiles for any unusual behaviour. If we keep an eye on our accounts, we can prevent any unwanted tracking or hacking. There are some women who simply don't care about the internet. When a check was written, he was discovered (Moore 2009). Nothing can be done to ignore this.

Internet cafés are a common place for us to use the web. Passwords and history of visited websites are recorded by public computer browsers. In order to proceed, please delete your browser's temporary and permanent files (Doyle 2012). The results of negligence can be catastrophic. Try to stay away from cyberstalkers at all costs. Firewalls, which are supposed to keep out hackers and strange websites, themselves can't visit sketchy ones. Personal firewall software is built into some operating systems by default.

The system is safe from harm when the computer is turned off. It is possible to limit cybercrime's effects (Cybercrimes Report 2012: 3-4). Everyone, regardless of gender, needs to be worried about cybercrime. Two sides exist to every story about the web, mobile tech, and the virtual world. Users can choose from a wide variety of available online protection options. The government of India ought to provide funding for studies of cybercrime. The criminal justice system benefits from increased education.

13. Conclusion

Cyberspace does not offer women the same level or range of desirable privacy as it does to men. Increasing numbers of computers and mobile devices are connecting to the Internet and exchanging information. Cyberspace has impacted our work, communications, and social interactions significantly by altering how consumers obtain information and form relationships.

Clearly, when data and other objects are transferred into cyberspace, numerous cybercriminal activities are also transmitted. New cybercrimes, such as those involving social networks, are emerging due to the rapid expansion of the amount of personal information that individuals communicate and post on the Internet, especially as the popularity of social networks rises. The law regulates cyberstalking, e-mail harassment, cyberbullying, morphing, email spoofing, and cyber defamation. Real-world consequences result from the user's awareness of the harm he or she has suffered in cyberspace. This dilemma is caused by a lack of knowledge in particular fields, which is exacerbated by the widespread availability of information technology. In a future study, we will investigate how education can reduce people's perceptions of cyber risks and, as a result, their fear of cybercrime. We cannot eradicate crime completely, but we can make our communities safer. Cybercriminals must be deterred by policymakers and law enforcement in a technologically dependent society. Technology has both advantages and disadvantages. Several laws address cybercrime against women. Government officials and legislators are responsible for ensuring that technological innovation is legal and ethical. As more individuals, particularly vulnerable women, utilise the Internet, criminal activity rises. In India, reports of online crimes against women are increasing. Teens engage in adultery, flirt, and start virtual fires. It is rational for Indian women to be concerned about negative media coverage. When women spend more time online without understanding the consequences, they are at risk. Never harass women online. Cybercrime is expanding concurrently with cyberlaw. Cyberspace law must address these online dangers. Governments and cyber law organisations must be informed immediately. India funded internet trends research in 2013 and 2014. In 2014, India hosted a conference on cyber law. These programmes enhanced global and intellectual cooperation. Despite having few cyber courts, India's police force is well-trained. Cybercriminality has not decreased.