International Research Journal of Commerce and Law
Volume 13 Issue 03, March 2025 ISSN: 2349-705X Impact Factor: 8.893
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

CYBER CRIMES AGAINST WOMEN IN INDIA

Dr. Munesh Kumar
Assistant Professor of Law
Govt. P.G. College, Sikar (Rajasthan)
E-mail id – kumarmunesh09@gmail.com

1. INTRODUCTION

In recent years, cyberspace has become an integral part of our daily lives, and with the increasing use of technology, cybercrime has emerged as a significant threat to society. Cybercrime refers to illegal activities that are carried out using the internet or any digital technology. Cybercrime includes a broad range of offenses, from financial fraud to cyber bullying, hacking, and online harassment. Unfortunately, women have been disproportionately affected by cybercrime in India, where cyber offenses against women have increased rapidly in recent years.

Cybercrime has severe consequences for women in India, both in terms of mental and physical health. With the rise of social media and online platforms, cyber bullying and online harassment have become widespread in India, targeting women in particular. Women face cyber threats like stalking, identity theft, and revenge pornography, leading to severe mental distress and emotional trauma. According to a study by the National Commission for Women, 54.8% of women have experienced cyber harassment, while 26% of them have reported cases of morphed images or videos. Moreover, cybercrime has also had a significant economic impact on women, with many women losing their jobs or experiencing financial losses due to online fraud.

The different types of cybercrimes against women in India include online harassment, cyber bullying, online stalking, revenge pornography, and cyber financial fraud. Online harassment involves sending threatening or offensive messages or comments on social media platforms, while cyber bullying is the use of technology to harass, humiliate, or intimidate someone. Online stalking is a pattern of repeated online harassment that involves following, monitoring, or tracking someone's online activity. Revenge pornography involves the distribution of sexually explicit images or videos without the victim's consent, while cyber financial fraud includes online phishing, credit card fraud, and other forms of online financial scams.

The current state of cyber security in India is a cause for concern, with India ranking among the top five countries in the world for cybercrime. Despite the government's efforts to strengthen cyber security laws and regulations, there are still significant gaps in implementing cyber security measures in India. The lack of awareness and knowledge about cyber security among the general public and law enforcement agencies also exacerbates the problem. Moreover, the increasing use of technology and the internet has led to an increase in the number of cybercrimes, making it challenging to address the issue effectively.

Cybercrime against women in India is a growing concern, with severe consequences for women's mental and physical health, as well as their economic wellbeing. The different types of cybercrimes, including online harassment, cyber bullying, online stalking, revenge pornography, and cyber financial fraud, require immediate attention from the government, law enforcement agencies, and civil society organizations. There is a need for a comprehensive approach to addressing cybercrime, including increasing public awareness, strengthening cyber security laws and regulations, and providing support to victims of cybercrime.

2. MEANING OF CYBERCRIME

Information Technology Act of 2000 or any other law in India does not mention cybercrime. A crime or offense has been precisely defined by a list of specific offenses and the penalties that go along with them under The Bharatiya Nyaya Sanhita (BNS) 2023, and a number of other statutes. As a result, cybercrime may be described as a synthesis of technology and crime. Cybercrimes are simply, "any offense or crime that involves the use of a computer."

Cybercrime is the term used to describe crimes carried out online in which the perpetrator remains anonymous behind a computer screen and is not necessarily required to make eye contact with the victim. In a cyber-crime, the computer or the data is the intended victim, the crime's intended outcome, or a tool used to facilitate the commission of another crime by providing the required inputs. The term "cybercrime" broadly refers to all of these offenses.

3. DIFFERENT CYBER CRIMES TARGETING WOMEN

(a) Hate Speech: In Social Media women actively express their views and opinions on various issues, political, religious or otherwise and become target of verbal abuse or criticism by certain group(s) of people. Citron mentioned this group attack as "Cyber Mob Attack"1. In India, the freedom of speech is a fundamental right guaranteed under the Constitution of India. However, the freedom of speech does not entitle anyone to use abusive language against another, whether it is offline or in online space. Section 66A of the Information Technology Act, 2000 which now stands struck down by the Supreme Court in the Shreya Singhal2 case, had prescribed punishment for sending offensive messages through communication service. The said provision was however struck down due to ambiguity in its words (such as 'grossly offensive or menacing character') which allowed its gross abuse or misuse.

(b) Sexual harassment on social media: Women may be contacted by other women or men for discussing any tropic of interest. It is often seen fake user IDs are created by men to grab a fake identity and pose as women or children or garb an identity to look younger or the older than the actual age. The motive behind such acts can be to carry out sexual harassment through writing such remarks, sexual favors or show pornography against the will of a woman. Such acts are punishable with an imprisonment which may be extended upto 3 years or fine or both Under BNS. The offence is cognizable, bailable and triable by any Magistrate.

(c) Voyeurism: A person expects privacy in certain areas – washroom, changing areas in malls and in one's own bed room. However, it is shocking to see rampant privacy invasions through use of hidden web cameras frequently reported in news reports3. Section 77 of the Bharatiya Nyaya Sanhita (BNS) 2023 prohibits the act of voyeurism, that is, where

[1] Citron, 2009
[2] AIR 2015 SC 1523
[3] Police hunt man who placed hidden camera in Starbucks toilets after he accidentally filmed himself installing it, The Independent, http://www.independent.co.uk/news/uk/crime/starbucks-hidden-camera-voyeur-pervert-vauxhall-metropolitan-police-lambeth-london-a8068736.html

someone watches or captures the images of a woman engaging in a private act where she would expect not being observed by the cyber criminal or publishes or transmits such images to a third person.

(d) Cyber Stalking: A woman may be stalked in social forums, social media or even by installing a key logger which enables a criminal to see everything she types online. Before Section 66A was struck down, IT Act, 2000 contained a specific provision prohibiting the cyber stalking. Section 66A(b) prohibited the act of sending an information which one knows is false but to cause annoyance, inconvenience or danger or to obstruct, intimidate a woman sends such information persistently through a computer or communication device such as mobile phone. This is a form of positive cyber stalking where the person who is stalked knows she is stalking.

(e) Sending obscene content: Sometimes women may receive unsolicited calls and obscene video or images which are obscene in nature from a stranger or a known person. Such acts are also punishable under the extant law in India. Section 67 of the Information Technology Act, 2000[4] prohibits the act of publishing or transmitting any material which is obscene in nature and makes act punishable with imprisonment of upto 3 years and fine upto Rs.5.00 Lacs and in the event of second conviction with imprisonment for a term which may extend upto 5 years and fine upto Rs.10.00 Lacs.

(f) Cyber Defamation: In case any person is defamed online/offline, that, is one's reputation is injured by words spoken or written which is published or transmitted to another person, it is a punishable offence. Victim can seek civil remedy of claiming damages and in criminal remedy seek punishment for offender.

(g) Morphing: - The term of 'Morphing' means to use photograph of a person from the personal pictures posted by the person on internet or clicked by a person and changing the contents using some part of the picture using software. Software that allows morphing could be

[4] The section criminalizes publishing or transmitting material that is "lascivious" or appeals to "prurient interest," or if its effect is to tend to "deprave and corrupt" people who are likely to read, see, or hear it.

misused to create obscene pictures of women where certain parts of the pictures are juxtaposed by using another picture. Such acts may constitute fabrication under Bhartiye Nyay Sanhita.

(h) Identity theft: A number of cases have been reported where fake profiles of women have been created on social media using their genuine pictures illegally used from the internet. This constitutes the offence of 'identity theft' which is punishable under Section 66C of the Information Technology Act (Hereinafter referred to as 'IT Act'). Any person who fraudulently or dishonestly makes use of the electronic signature, pass word or other unique identification feature e.g. photograph of a person without his consent is punishable with imprisonment for a term upto 3 years and fine upto 1.00 Lac.

(i) Spamming: The erstwhile Section 66A of the I.T. Act prohibited the offence of spamming which means sending any unsolicited messages to a person to cause annoyance, inconvenience or to mislead the recipient about the origin of the message. Such acts were punishable with upto 3 years imprisonment and fine. However, after such provision was struck down in the Shreya Singhal versus Union of India[5] by the Supreme Court of India, there is no specific provision to deal with spamming in India.

(j) Cheating by impersonation: In many cases specially on matrimonial sites fake profiles of men are posted where women may be cheated due to impersonation. A man who is married may portray to be unmarried and cheat a woman whom he promised to marry. In such cases, Section 66D of IT Act,2000 prescribes punishment for cheating by personation using a computer resource with imprisonment for a term which may extend upto 3 years and liable to fine upto Rs.1.00 Lac.

(k) Virtual rape: Threatening to rape her and encourage other members to comment on his post. This would attract punishment for offence under Section 75 of the BNS and under provisions of the Section 4 of the Indecent Representation of Women (Prohibition) Act, 1986. Section 4 of the Indecent Representation of Women (Prohibition) Act,1986 prescribes punishment of upto 2 years,

[5]AIR 2015 SC 1523

fine or both for publishing, sending any message containing indecent representation of women. In many cases cyber victimization of a woman could occur where offender posts vulgar messages

(l) Cyber bullying: When a harasser intimidates a woman online she is said to be cyber bullied. Though men are also cyber bullied, women typically are targeted for example, just after an emotional break up or as domestic violence or as modus operandi of by an offender.

(m)Revenge porn: In many cases, when a relationship between a man and woman gets estranged, the ex-friend or the ex-husband may post or publish pictures or video which are personal in nature and unauthorisedly circulate it to the targeted woman and her close friends. This is known as sending of revenge porn. There is no express provision using this term under the I.T. Act but it has provisions that can apply in this context. Sections 67 and 67A of the I.T. Act discussed hereinbefore and Section 335 of the BNS may apply. Even in case where the woman consents to the capture of images but not to their dissemination to third party, such dissemination is considered as offence punishable with imprisonment for a term not less than one year but may extend to 3 years.

(n) Domestic violence through verbal abuse: In many cases where a man or women are experiencing relationship difficulties, one may vent out anger against the other on social media. Depending on the content of the message, if it contains sexual abuse, it may constitute sexual harassment under Section 75 of the BNS or act to outrage modesty of a woman under Section 79 of BNS.

(o) Extortion: Cybercriminals may employ phishing technique to make unlawful financial gains or send phishing emails posing as if the mail has been sent by a genuine bank. Such mails are fake and sent with a view to unauthorisedly extract the personal sensitive information about one's Credit Card or net-banking details. A phisher could then rob one of monies and may even install viruses and steal data such as personal pictures and later extort the victim to get monies or sexual favours. This is known as sextortion. Extortion is an offence under the Bharatiya Nyaya Sanhita (BNS), 2023 under Sections 308 punishable with imprisonment upto 7 years or fine or both.

(p) Breach of Data: Where personal sensitive data of a woman is stolen by a person fraudulently or dishonestly it will fall under Section 66 of the I.T. Act r/w Section 43 of the I.T. Act, 2000 punishable with term of imprisonment of upto three years, fine or both. However, if such data is taken by a person who is authorized by the I.T. Act to collect such information and he without the

consent of the person discloses such information, such act is punishable with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs.1.00 Lac or both.

4. CAUSES OF CYBER CRIMES AGAINST WOMEN

Cyber crimes against women in India are a complex phenomenon that is influenced by several underlying factors. These factors include gender-based violence, patriarchal attitudes, and lack of awareness about cyber security. Gender-based violence is a root cause of cyber crimes against women in India. Women in India face various forms of violence, such as domestic violence, sexual harassment, and physical assault. These forms of violence often spill over into cyberspace, where perpetrators use technology to harass, stalk, or blackmail their victims. In many cases, the perpetrators are known to the victims, such as intimate partners or family members. According to a report by the National Crime Records Bureau[6], over 93% of rape cases in India were committed by someone known to the victim.

Patriarchal attitudes in Indian society also contribute to the prevalence of cyber crimes against women. The patriarchal system promotes male dominance and control over women, leading to a culture of misogyny, victim-blaming, and discrimination. These attitudes often manifest in cyberspace, where women are subjected to online harassment, trolling, and abuse. Women who speak up against harassment or violence are often accused of bringing shame to their families or communities. The lack of support from family and society can deter women from reporting cyber crimes.

The lack of awareness about cyber security is another contributing factor to the prevalence of cyber crimes against women in India. Many women in India lack basic knowledge about safe online practices, such as creating strong passwords, avoiding phishing scams, and using privacy settings. This lack of awareness makes them vulnerable to cyber attacks, such as identity theft,

[6] The National Crime Records Bureau (NCRB) is an Indian government agency responsible for collecting and analyzing crime data, as defined by the Bhartiye Nyay Sanhita (BNS) and Special and Local Laws (SLL).

financial fraud, and data breaches. The absence of comprehensive cyber security policies and laws also makes it difficult for women to seek justice and protection.

i. In 2020, a woman in Delhi was harassed and threatened with revenge porn by her former partner, who was angry about their breakup. The woman did not report the incident due to fear of retaliation and lack of support from her family.

ii. According to a report by the National Family Health Survey, over 30% of women in India have experienced physical or sexual violence by their intimate partners.

iii. A survey by the Internet and Mobile Association of India found that only 30% of women in India use strong passwords, while 60% share their passwords with others.

iv. According to a report by the National Crime Records Bureau, there were over 4,000 cases of cyber crimes against women in India in 2019.

The prevalence of cyber crimes against women in India is a complex issue that requires a multi-pronged approach to address. It is essential to address the underlying factors that contribute to the problem, such as gender-based violence, patriarchal attitudes, and lack of awareness about cyber security. This can be achieved through policy reforms, education and awareness programs, and community-based interventions. It is also crucial to provide support and protection to women who are victims of cyber crimes, through legal aid, counselling, and other support services.

5. CYBER CRIME LAWS IN INDIA:

The rise of cyber crimes against women in India has led to the development of a legal framework to address these crimes. The legal framework in India includes several laws and regulations, including the Information Technology Act, 2000[7], The Bharatiya Nyaya Sanhita (BNS) 2023, and the Protection of Women from Domestic Violence Act, 2005. Let's take a closer look at these laws and regulations

[7] Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

The Information Technology Act, 2000 (IT Act) is the primary law that deals with cyber crimes in India. The IT Act was enacted to provide legal recognition for electronic transactions and to facilitate e-governance. The IT Act includes provisions that deal with cyber crimes against women, such as hacking, identity theft, and electronic stalking. The IT Act also provides for the establishment of cyber crime investigation cells in every state to investigate and prosecute cyber crimes.

The Bharatiya Nyaya Sanhita (BNS) 2023[8] is the primary criminal law in India. The BNS includes provisions that deal with crimes against women, such as rape, sexual harassment, and domestic violence. The BNS has been amended to include provisions that deal with cyber crimes against women, such as voyeurism, cyber stalking, and dissemination of sexually explicit material. The BNS also provides for punishment for abetment to cyber crimes against women.

The Protection of Women from Domestic Violence Act, 2005[9] (PWDVA) is a civil law that provides protection to women who are victims of domestic violence. The PWDVA defines domestic violence broadly to include physical, sexual, verbal, emotional, and economic abuse. The PWDVA also includes provisions that deal with cyber crimes against women, such as online harassment, stalking, and revenge porn. The PWDVA provides for protection orders, residence orders, and monetary relief to women who are victims of domestic violence.

- In 2019, a man was sentenced to two years in jail for stalking a woman on social media. The man had created fake profiles on social media to harass the woman and had also threatened to upload her private pictures online.
- According to a report by the National Crime Records Bureau, there were over 4,45,256 cases of crime against women were registered in 2022, an increase of 4% compared to 4,28,278 in 2021.

[8] The official criminal code of India, It came into effect on July 1, 2024, after being passed by Parliament in December 2023, replacing the Indian Penal Code.
[9] Act of the Parliament of India enacted to protect women from domestic violence. The law came into force on 26 October 2006.

- In 2018, the Supreme Court of India upheld the constitutional validity of Section 66A of the IT Act, which deals with the punishment for sending offensive messages through communication services. The Court held that Section 66A was necessary to protect the dignity of women and prevent cyber harassment.

The legal framework in India that deals with cyber crimes against women is a critical tool to provide protection and justice to women who are victims of cyber crimes. The framework includes several laws and regulations, such as the Information Technology Act, Bharatiya Nyaya Sanhita, and Protection of Women from Domestic Violence Act. However, the implementation of these laws and regulations remains a challenge, and there is a need for capacity building of law enforcement agencies and the judiciary.

6. CHALLENGES IN ADDRESSING CYBER CRIMES AGAINST WOMEN

Cyber crimes against women in India are a growing concern, and efforts to address them are complicated by a number of challenges. In this section, we will explore some of the key challenges that law enforcement agencies and the legal system face in addressing cyber crimes against women in India.

One of the main challenges is the lack of resources available to law enforcement agencies to investigate and prosecute cyber crimes. Cyber crimes are often complex and require specialized knowledge and technology to investigate. However, many police departments in India are understaffed and lack the necessary resources to handle cyber crime cases effectively. This can result in delayed or inadequate investigations and low conviction rates.

Another challenge is the low reporting rate of cyber crimes against women. Many women may not report incidents of cyber crimes due to fear of retaliation or social stigma, or because they are not aware of their rights or the available legal remedies. This underreporting can make it difficult for law enforcement agencies to accurately assess the prevalence of cyber crimes against women and allocate resources accordingly.

In addition, the legal system in India faces challenges in addressing cyber crimes against women. The Indian Penal Code and the Information Technology Act, 2000, provide legal provisions for cyber crimes, but they may not always be effectively implemented or enforced. There may also be a lack of clarity or inconsistencies in the interpretation of these laws, which can result in different outcomes for similar cases.

Finally, the lack of adequate training for law enforcement officials and legal professionals can be a significant challenge in addressing cyber crimes against women. Many law enforcement officials may not have the necessary knowledge or skills to handle cyber crime cases, and legal professionals may not have specialized training in cyber crime law. This can lead to errors in investigations or legal proceedings, and can contribute to low conviction rates.

7. BEST PRACTICES FOR PREVENTING CYBER CRIMES AGAINST WOMEN

Cyber crimes against women in India are on the rise, and it is crucial for women to take measures to protect themselves from becoming victims. some best practices that women can follow to prevent cyber crimes against themselves.

- **Use Strong Passwords**: One of the simplest yet most effective ways to protect yourself from cyber crimes is to use strong passwords. Make sure your passwords are at least 12 characters long and include a mix of upper and lowercase letters, numbers, and special characters. Avoid using easily guessable passwords like your name, date of birth, or pet's name.

- **Keep Personal Information Private**: Be careful about what personal information you share online, including on social media platforms. Avoid sharing your phone number, home address, or other sensitive information publicly. Also, be wary of phishing emails or phone calls asking for personal information.

- **Be Careful with Social Media**: Social media can be a double-edged sword. While it can help you stay connected with friends and family, it can also be a breeding ground for cyber

crimes. Be cautious of whom you add as friends, and avoid sharing personal information or sensitive photos online.

- **Use Two-Factor Authentication**: Two-factor authentication adds an extra layer of security to your online accounts by requiring a second form of authentication, such as a code sent to your phone, in addition to your password. Many popular online services, including email providers and social media platforms, offer this feature.

- **Keep Software Up-to-Date**: Make sure to keep your software, including your operating system and antivirus software, up-to-date. Software updates often contain security patches that address vulnerabilities that cyber criminals may exploit.

- **Use Antivirus Software**: Antivirus software can help detect and prevent malware and other malicious software from infecting your device. Make sure to install reputable antivirus software and keep it up-to-date.

- **Report Incidents**: If you become a victim of cyber crime, it is crucial to report the incident to the authorities. Reporting incidents can help prevent future crimes and can also help law enforcement track down and prosecute cyber criminals.

8. CONCLUSION:

The Internet has the ability to empower everyone at the start of the new millennium by providing them with access to knowledge and social support regarding their concerns about their physical and mental health as well as by promoting digital advocacy for shifts in societal and organizational policy. However, there are dangers and potential dangers that must be addressed. Online victimization can be brought on by incomplete information, invasion of privacy, restricted communication, online harassment, and cyberstalking. If the potential of the Internet to deliver services is to be realized, users both individuals and other institutions and e-commerce sites must comprehend and protect against these risks. Taking precaution and education about online safety and privacy issues are important but not the end. Laws of a nation often reflect its social and moral values and have social conduct rules. Over the years technological advancement has taken up with a rapid speed and has increased the

number of users of the internet, computer and mobile phones, it has change faster than the laws governing them. It has created a wave of opportunities for many people, but it's often a curse for many who have been victimized by it in any form.

Cyber-crimes are immoral and can harm the reputation of victims to a great extent but many countries only recognise the sexual aspect of such cyber-crimes against women particularly and do not value cyber-crimes of non-sexual types. Countries still need to move away from the social aspect of laws that are framed to combat such crimes and give proper protection. Due to fear of reputation and other social stigma attached to their family such crimes are often less recognised and reported out in the public. There is a lack of awareness on the part of the public as well as investigating officers and cyber cells. They often don't know how to react and act when such incidents have taken place and victim comes for help. We recognise that the primary cause of the low reporting rates and nearly nonexistent use of the laws intended to address offences other than obscenity and pornography is a lack of understanding among the general public, particularly among female victims. Laws often just prescribe punishment like imprisonment, fine or damages to the victim. The law should look beyond this. They should be looking out for victim welfare and how to resynthesize them back in society if they have been suffering from the trauma of cyber-crimes. The police officer or the cyber cell or trial judge could do much more by ordering the removal of the online material posted or shared by anyone without such person’s consent. Police officers should be given training to handle such cases and there should be cyber cell officers in every police station. There should be cyber hotlines for sharing such grievances. Reputation management techniques and modal conduct should be taught which can help victims overcome his fear.

Furthermore, it must be kept in mind that cyber victimization cannot be stopped by simply imposing fines or jail terms as penalties. Online service providers like Whatsapp, Google, Yahoo, Facebook, Instagram and Twitter, which are actually based in the US, are almost completely irresponsible when it comes to tracking subscribers' online activity through the creation of false identities and the use of social media or other websites to harass victims even more. People and students must be given general training and know how to use such apps and software for protecting them from such crimes and reporting them to the requisite authorities.

Thus the internet is a boon or bane that depends on how one uses it. It may offer endless opportunity and attraction but one must always be aware of their rights and privacy and know how to use such apps and technologies in the greatest positive manner.

In conclusion, cyber crime against women in India is a serious issue that requires collective efforts from the government, law enforcement agencies, technology industry, and society at large to address effectively. With the right approach and collaboration, we can create a safe and secure cyberspace for women in India.