THE LAWWAY WITH LAWYERS JOURNAL

VOLUME:-24 ISSUE NO:- 24 ,JUNE 29, 2025

ISSN (ONLINE):- 2584-1106

Website: www.the lawway with lawyers.com

Email: thelawwaywithelawyers@gmail.com

Authored By :- Priya Kumari,

a student at Central University of South Bihar, Gaya

CYBER CRIME AGAINST WOMEN

Abstract

In the era of rapid digitalization, cyber crime against women has emerged as a growing and deeply concerning issue. With increasing access to the internet and social media, women are frequently subjected to online threats such as cyberstalking, cyberbullying and non-consensual sharing of private content etc. These acts not only infringe upon women's right to privacy and dignity but also have long-lasting psychological and social consequences. Despite existing legal provisions in India like the Information Technology Act, 2000 and sections of the Indian Penal Code, enforcement remains weak and awareness among victims is low. This article explores the nature, causes, and impact of cyber crime against women, highlighting the urgent need for stronger legal frameworks, digital literacy, and gender-sensitive law enforcement to ensure a safer online space for all.

Keywords: Cybercrime, cyberbullying, cyberstalking, sextortion

Preface

Cyberspace is the name given to the computer- generated world of the internet, and cyber laws are the regulations that apply there. Due to the fact that this space has a form of universal governance, all druggies are governed by these regulations. Cyber law is another area of law that deals with legal problems brought on by the operation of networked information technology. People each across the world have been going through delicate times because of the epidemic.

Another catastrophe, videlicet cybercrime and mobile crime, spread like a contagion while people defied and fought the epidemic. Several people expressed their annoyance with the lockdown by abusing the internet and phone technologies and plaguing others, while numerous used these means to keep themselves distracted and engaged throughout the outbreak. During the outbreak, internet- grounded cybercrime grew fleetly and intensely.

Meaning of Cybercrime

Information Technology Act of 2000 or any other law in India doesn't mention cybercrime. A crime or offense has been precisely defined by a list of specific offenses and the penalties that go on with them under the Indian Penal Code, 1860, and a number of other bills. As a result, cybercrime may be described as a conflation 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 isn't inescapably needed to make eye contact with the victim. In a cyber-crime, the computer or the data is the intended victim, the crime's intended outgrowth, or a tool used to grease the commission of another crime by furnishing the needed inputs. Cybercrime Victims Women and children were the most vulnerable corridor of society during the epidemic, making them simple targets for cybercriminals whereas men and grown-ups were victims of several cybercrime swindles. Women were exposed to these crimes during the epidemic, in particular housewives and those who use social media. The data from the 2021 National Commission for Women show that after a lockdown, the number of cybercrime incidents against women decreases. When India was poorly affected by the alternate batch of COVID- 19 and nearly the entire country was subordinated to rigorous lockdown restrictions in April and May of 2021, the frequence of cybercrimes against women increased drastically in March and continued to rise. Eventually, after the alternate epidemic surge passed and the lockdown restrictions were released in June, the frequence of cyber-attack circumstances started to dwindle as well. This script lasted till July as the lockdown restrictions were lifted. In earlier times, there were veritably many womanish victims of cybercrime, but during the epidemic and lockdown, this figure significantly increased.

Women as the Victim of Cybercrimes

During the epidemic and lockdown, people were impelled to use the internet for social, professional, recreational, and educational purposes. Through the use of laptops, smartphones, and the internet, working women started working from home. Women who are still in academy are impelled to use the internet for online coursework and other academic hobbies. The rate of cybercrime against women started to increase at this time since the maturity of women were using social media spots and one or further online platforms for academic, professional, and entertainment purposes. culprits started mentally and emotionally plaguing the victim because they couldn't physically harm them because the entire country was on lockdown.

Women are most generally exposed to the following Cyber Crimes

Sextortion: The most common cybercrime performed against women during the epidemic was sextortion. By using their victims' private prints or altered images as blackmail, the malefactors started demanding plutocrat or sexual favors from them. In order to express their aggravation about the epidemic, the malefactors hovered women and asked for sexual videoconferencing or letters from them. also, as they had no plutocrat, they felt empowered to hang victims with their altered images in order to get plutocrat from them. Phishing To make plutocrat during the lockdown, culprits shoot fake- mails with a link to a particular webpage in an trouble to force the victim into entering particular information like contact details and watchwords or with the purpose of infecting the victim's device with dangerous contagions as soon as the link is clicked. These textbooks and emails appear to be authentic. The bushwhackers also carry out shady deals from the victim's bank account to their own using the victim's bank account and other private information. Pornography During the epidemic, malefactors indulged in online sexual attacks against women, altering the victim's image and using it in pornographic material.

Cyber stalking: It included, among other effects, reaching or trying to engage the victim via social media spots or phone exchanges despite her egregious lack of interest, posting dispatches on the victim's runner(frequently hanging in nature), and persistently bothering the victim with emails and phone calls. Cyber playing During the epidemic, people started reading the news online. There are further exemplifications of false news and information now than ever ahead. After clicking on vicious URLs, the women were the victims of cyber hacking. The malware downloaded all of their particular information to their phones, turned on the microphone and camera, and took their intimate prints and vids. also, culprits use these bits of information and filmland to carry out highway robbery and other offenses.

Cyber-bullying: This includes, transferring rape and death pitfalls to the victim and posting false, deceiving, and vituperative statements about the victims on social media spots, and demanding plutocrat to have them removed. It also includes leaving hurtful commentary on the victim's posts. A computer, cell phone, or laptop are exemplifications of digital or communication technology that are used for importunity and bullying.

Cybersex trafficking: It’s different from physical coitus trafficking in that the victim doesn’t physically engage with the perpetrator. Cybersex trafficking is when a dealer broadcast records, or takes filmland of the victim engaging in sexual or intimate conditioning from a central position and also sells the content online to sexual bloodsuckers and guests. The culprits has forced, Manipulated, and blackmailed women into sharing in cybersex trafficking, which constitutes sexual abuse of women.

Legal vittles

Although a full nonsupervisory frame for laws regulating the cyber sphere, including similar conditioning, has not been drafted, certain legal remedies under colorful bills can help a victims

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

Section 354A says that a man who commits any of the following events – a demand or plea for sexual services; or displaying pornography against a woman's will; or making sexual reflections – commits sexual importunity and may be punished with strict imprisonment for a period up to 3 times, or with a fine, or with both. In the case of the first two, and with a period of imprisonment for a period of over to one time, or by a fine, or with the both.

Section 354C defines ' voyeurism ' as the act of shooting and/ or publishing a picture of a woman engaged in a private act without her concurrence. To qualify as ' Voyeurism, ' the conditions must be similar that the lady would " generally anticipate not to be seen, either by the lawbreaker or by any person acting at the perpetrator's direction. " A person condemned underneath this section faces a fine and over to three times in captivity on the first conviction and 7 times on consecutive persuasions.

Section 354D added a stalking prohibition that includes online stalking. Stalking is described as an act in which a manly pursues or connections a woman despite the woman's apparent objectiveness in similar contact, or watches a woman's cyber exertion or operation of the Web or electronic communication. A man condemned of stalking faces up to three times in captivity and a fine for the first offence, and over to five times in captivity and a fine for consecutive persuasions. Piecemeal from the specific variations to the Code, there are a number of other laws within which cyber-attacks may be reported and the indicted fulfilled. These include the following-

Section 499 To libel, someone is to commit an act with the thing of vilifying their character. When committed with the intent to injure the woman's character, vilification through the publishing of immediate and clear representation of insinuation is penalized with imprisonment for a period not exceeding two times, a fine, or both.

Section 503 pitfalls to harm a person's character, either to beget her fear or to impel her to modify her course of conduct about whatever she'd typically do not do, constitute felonious intimidation. The act of cyber-blackmailing a person, as was done in the forenamed illustration, can be placed within the range of this law.

Section 507 This section establishes the maximum penalty for Felonious Intimidation committed by an individual whose identity is unknown to the victim. Any anonymous communication that constitutes felonious intimidation in violation of the antedating Section 503 is punished under this section.

Section 509 Any existent who utters a word, makes a sound or gesture, or displays an object with the intent that similar word, sound, gesture, or object is heard or seen by a womanish and

insults her modesty, or intrudes on her sequestration, may be charged underneath this section and doomed to over to three times in captivity and a forfeiture. This section may correct cases of sexual reflections or commentary made over the Net, as well as other unequivocal prints and content that are forcefully transmitted over the web.

The Information Technology Act 2000

Section 66C Identity theft is a crime that's punishable under Section 66C of the IT Act. This provision would be applicable to scripts of cyber hacking. According to this clause, whoever falsely or dishonestly uses another person's electronic hand, word, or other distinctive relating point risks up to three times in captivity and a forfeiture of over to Rs. 1 lakh.

Section 66E still, addresses that issue, If someone's right to sequestration is traduced. A person can face up to three times imprisonment and/ or a fine for taking, participating, or transferring a picture of their private area without their concurrence or in a way that violates their sequestration. Section 67 stag content mustn't be published, transmitted, or made to be distributed under Section 67, which carries a maximum judgment of three times imprisonment or a fine for a first conviction and up to 5 times imprisonment and a fine for the alternate.

Section 67A Publishing, transmitting, or abetting in the transfer of sexually unequivocal material is a misdemeanor under Section 67A, punishable by over to five times in captivity and a fine for a first conviction and up to seven times of imprisonment and a fine for the posterior conviction.

Affiliated data

As of 2019, the total cybercrime incidents have gone up by18.4 but the number of cybercrime cases against women has gone up by 28, as shown by National Crime Record Bureau. Data showed that 10,730 incidents, or20.2 of the 52,974 incidents registered in 2021, were reported as crimes against women. In 2021, Karnataka had the largest share of cases(2,243), followed by Maharashtra(1,697) and Uttar Pradesh(958). The conviction rate or chance of case disposal by courts for cybercrime against women is lower than the conviction rate of cybercrime cases. Though the chance is still lower, it jumped up thrice between 2019 and 2021. That means the conviction rate went up from10.8 percent in 2019 to35.2 percent in 2021.

NCRB Report on Cybercrime

All Forms of Cybercrime A aggregate of 52,974 cases were registered under Cyber Crimes which shows an increase of5.9 in enrollment over 2020(50,035 cases in 2020), and if compared with 2019 data, the number of cybercrime incidents in 2021 has gone up by18.4 percent. Still, it increased from 3, If we talk about the share of the crime rate under total conducted crimes.7 in 2020 to3.9 in 2021. The maturity of cybercrime incidents reported in 2021(32,230 out of 52,974) had fraud as their primary provocation, followed by sexual exploitation(8.6; 4,555 cases) and highway robbery(5.4). still, Telangana reckoned for the biggest chance of cybercrime cases overall, with cases rising 282 from 2,691 in 2019 to 10,303 in 2021. The other four countries

with the most cases were Uttar Pradesh(8,829), Karnataka(8,136), Maharashtra(5,562), and Assam(4,846).

Cases

Shankar v State(2010)

Fact: The supplicant approached the Court under Section 482, CrPC to quash the charge distance filed against him. The supplicant secured unauthorized access to the defended system of the Legal Advisor of Directorate of Vigilance and Anti-Corruption(DVAC) and was charged under Sections 66, 70, and 72 of the IT Act. Decision The Court observed that the charge distance filed against the supplicant can not be quashed with respect to the law concerning non-granting of permission of execution under Section 72 of the IT Act.

Shreya Singhal v UOI (2013)

In the instant case, the validity of Section 66A of the IT Act was challenged before the SC.

Fact: Two women were arrested under Section 66A of the IT Act after they posted allegedly obnoxious and reprehensible commentary on Facebook concerning the complete arrestment of Mumbai after the demise of a political leader. Section 66A of the IT Act provides discipline if any person using a computer resource or communication, similar information which is obnoxious, false, or causes annoyance, vexation, peril, personality, abomination, injury, or ill will. The women, in response to the arrest, filed a solicitation challenging the constitutionality of Section 66A of the IT Act on the ground that it's violative of the freedom of speech and expression.

Decision: The Supreme Court grounded its decision on three generalities videlicet discussion, advocacy, and incitement. It observed that bare discussion or indeed advocacy of a cause, no matter how unpopular, is at the heart of the freedom of speech and expression. It was set up that Section 66A was able of confining all forms of communication and it contained no distinction between bare advocacy or discussion on a particular cause which is obnoxious to some and incitement by similar words leading to a unproductive connection to public complaint, security, health, and so on.

Suggestions for or precluding Cybercrime

- Watch out for meaningless or fraudulent phone or dispatch dispatches.
- Emails that request particular information shouldn't be replied to.
- Watch out for fraudulent websites that try to gain your particular information.
- Pay special attention to the sequestration programs that are included with the software and posted on websites.
- Make sure your dispatch address is secure.
- Put Secure watchwords to use.

- A victim of cybercrime should notify the original cyber cell or a police station.
- A complaint can also be submitted anonymously through the National Cybercrime Reporting Portal.

Conclusion

Particularly in an decreasingly technologically reliant world, crime related to electronic law-breaking is certain to increase, and lawmakers must go the redundant afar to keep hoaxers at bay. Technology is frequently a double- whetted brand that can be employed for either good or evil purposes. A number of laws have been passed by the legislative to address cybercrime against women. In order to insure that technology advances in a healthy way and is used for legal and ethical profitable growth rather than illegal conditioning, autocrats and lawmakers should work continuously to achieve this.

References

https://www.legalserviceindia.com

https://www.blogipleader.in

https://enhelion.com

https://ncw.nic.in