IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBER CRIME AGAINST WOMEN IN INDIA

Ms.Nivedita Diwate

ASSISTANT PROFESSOR

Karnataka State Law University

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 jurisdiction, all users are governed by these regulations. Cyber law is another area of law that deals with legal problems brought on by the usage of networked information technology. People all across the world have been going through difficult times because of the pandemic.

The lack of healthcare services, the dissatisfaction and isolation that came with lockdowns, the loss of jobs and business income, and the loss of loved ones to this deadly sickness were just a few of the difficulties that people had to deal with. Numerous lives have been lost and millions of people have been affected by the COVID-19 epidemic, which has proven to be a catastrophe. In addition to the millions of deaths caused by the pandemic, it has also been a difficult time for many people who have lost their jobs or had to shut down their businesses because of lockdown, for families who have lost the only wage earner, for kids who have lost both parents at a young age, and for many others.

This is not the case, though! Another catastrophe, namely cybercrime and mobile crime, spread like a virus while people resisted and fought the pandemic. Several people expressed their annoyance with the lockdown by abusing the internet and phone technologies and tormenting others, while many used these means to keep themselves distracted and occupied throughout the outbreak. During the outbreak, internet-based cybercrime grew rapidly and intensively.

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 Indian Penal Code, 1860, 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.

The following are included in cyber law:

Cyber Criminals

Electronic And Digital Signatures

Protection Of Private And Personal Information

Intellectual Property

Cybercrime Victims

Women and children were the most vulnerable parts of society during the pandemic, making them simple targets for cybercriminals whereas men and adults were victims of several cybercrime scams. Women were exposed to these crimes during the pandemic, 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 badly affected by the second batch of COVID-19 and almost the entire country was subjected to rigorous lockdown restrictions in April and May of 2021, the frequency of cybercrimes against women increased drastically in March and continued to rise.

Finally, after the second pandemic wave passed and the lockdown restrictions were released in June, the frequency of cyber-attack occurrences started to diminish as well. This scenario lasted till July as the lockdown restrictions were lifted. In earlier years, there were very few female victims of cybercrime, but during the pandemic and lockdown, this figure significantly increased.

Women as the Victim of Cybercrimes

During the pandemic and lockdown, people were compelled 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 school are compelled to use the internet for online coursework and other academic pursuits.

The rate of cybercrime against women started to increase at this time since the majority of women were using social media sites and one or more online platforms for academic, professional, and entertainment purposes. Criminals started mentally and emotionally tormenting the victim because they could not physically harm them because the entire country was on lockdown.

Women are most commonly exposed to the following Cyber Crimes:

Sextortion:

The most common cybercrime performed against women during the pandemic was sextortion. By using their victims' private photos or altered images as blackmail, the offenders started demanding money or sexual favors from them. In order to express their aggravation about the epidemic, the offenders threatened women and asked for sexual

videoconferencing or letters from them. Additionally, as they had no money, they felt empowered to threaten victims with their altered images in order to get money from them.

Phishing:

To make money during the lockdown, criminals send fake e-mails with a link to a particular webpage in an effort to coerce the victim into entering personal information like contact details and passwords or with the purpose of infecting the victim's device with dangerous viruses as soon as the link is clicked. These texts and emails appear to be authentic. The attackers then carry out shady transactions from the victim's bank account to their own using the victim's bank account and other private information.

Pornography:

During the pandemic, offenders indulged in online sexual attacks against women, altering the victim's image and using it in pornographic material.

Cyber stalking:

It included, among other things, contacting or trying to engage the victim via social media sites or phone conversations despite her obvious lack of interest, posting messages on the victim's page (often threatening in nature), and persistently bothering the victim with emails and phone calls.

Cyber hacking:

During the pandemic, people started reading the news online. There are more examples of false news and information now than ever before. After clicking on malicious URLs, the women were the victims of cyber hacking. The malware downloaded all of their personal information to their phones, turned on the microphone and camera, and took their intimate photos and videos. Then, criminals use these bits of information and pictures to carry out extortion and other offenses.

Cyber-bullying:

This includes, sending rape and death threats to the victim and posting false, misleading, and abusive statements about the victims on social media sites, and demanding money to have them removed. It also includes leaving hurtful comments on the victim's posts. A computer, cell phone, or laptop are examples of digital or communication technology that are used for harassment and bullying.

Cybersex trafficking:

It is different from physical sex trafficking in that the victim does not physically engage with the perpetrator. Cybersex trafficking is when a dealer broadcasts, records, or takes pictures of the victim engaging in sexual or intimate activities

from a central location and then sells the content online to sexual predators and clients. The criminals have forced, manipulated, and blackmailed women into participating in cybersex trafficking, which constitutes sexual abuse of women.

Legal provisions regarding Cybercrime

Although a comprehensive regulatory framework for laws governing the cyber realm, including such actions, has not yet been developed, some legal remedies under different statutes can help victims of cyber violence.

The Indian Penal Code 1860

Before 2013, there was no law that dealt directly with cyberbullying or crimes committed against women online. Sections 354A to 354D are added to the Indian Penal Code, 1860 as a result of Section 354A of the 2013 Criminal Amendment Act.

Section 354A:

According to Section 354A, a male who engages in any of the following acts-demanding or pleading for sexual favors; showing pornography against a woman's will; or making sexual remarks-commits sexual harassment and may be punished with rigorous imprisonment for up to three years, a fine, or both. In the first two cases, there is a possibility of up to one year in imprisonment, a fine, or both.

Section 354C:

Voyeurism is defined in Section 354C as the act of taking a photograph of a woman engaging in a private act and/or publishing it without the lady's permission. The circumstances must be such that the woman would "usually expect not to be seen, either by the offender or by anyone else acting at the perpetrator's direction" for it to qualify as "voyeurism." If found guilty under this section, the offender may be fined and sentenced to up to three years in prison on the first conviction and seven years on subsequent conviction.

Section 354D:

The addition of Section 354D states about stalking prohibition that covers online stalking. The act of stalking is defined as when a man pursues or approaches a woman despite the woman's obvious disinterest in the interaction, or when a guy observes a woman's online behavior, use of the Internet, or electronic communication. If found guilty of stalking, a man might spend up to three years in jail and a fine, and subsequent convictions could land him in prison for up to five years and a fine.

In addition to the specific changes to the Code, there are a number of other provisions that provide for the reporting of cyber-attacks and the prosecution of those who are responsible.

These consist of the following:

Section 499:

To slander is to do something with the intent to harm someone's reputation. Defamation through the publication of an instant and unambiguous portrayal of imputation is punishable by up to two years in prison, a fine, or both when done with the intent to harm a woman's reputation.

Section 503:

Criminal intimidation occurs when a person is threatened with reputational injury in an effort to make her panic or force her to do what she ordinarily does or does not do. This rule can be applied to situations where someone is cyber-blackmailed, as was done in the aforementioned scenario.

Section 507:

This section specifies the maximum punishment for criminal intimidation done by a person the victim does not know. This clause sanctions any anonymous communication that violates Section 503's prohibition on criminal intimidation.

Section 509:

Anyone who speaks, gestures, shows an object, or makes a sound with the intent that it be heard or seen by a female and offends her modesty or invades her privacy may be charged with violating this section and punished with up to three years of imprisonment and a fine. This provision may impose penalties for instances of sexually explicit images and content that are forcibly distributed online, as well as for remarks or comments made in a similar vein.

The Information Technology Act 2000

Section 66C:

Identity theft is a crime that is punishable under Section 66C of the IT Act. This provision would be applicable to scenarios of cyber hacking. According to this clause, whoever falsely or dishonestly uses another person's electronic signature, password, or other distinctive identifying feature risks up to three years in prison and a fine of up to Rs. 1 lakh.

Section 66E:

If someone's right to privacy is breached, Section 66E addresses that issue. A person can face up to three years imprisonment and/or a fine for taking, sharing, or sending a picture of their private area without their consent or in a way that violates their privacy.

Section 67:

Obscene content must not be published, transmitted, or made to be distributed under Section 67, which carries a maximum sentence of three years imprisonment or a fine for a first conviction and up to 5 years imprisonment and a fine for the second.

Section 67A:

Publishing, transmitting, or aiding in the transfer of sexually explicit material is a misdemeanor under Section 67A, punishable by up to five years in prison and a fine for a first conviction and up to seven years of imprisonment and a fine for the subsequent conviction.

Indecent Representation of Women Bill 2012

Obscene depictions of women in publications, advertising, and other media are prohibited by this Bill. With the passage of this bill, the legal framework will be expanded to cover electronic and audiovisual media, as well as the distribution of information online and the representation of women on the internet. But as of July 2021, this Bill has been withdrawn.

Suggestions For Preventing Cybercrime:

Watch out for pointless or fraudulent phone or email messages.

Emails that request personal information should not be replied to.

Watch out for fraudulent websites that try to obtain your personal information.

Pay special attention to the privacy policies that are included with the software and posted on websites.

Make sure your email address is secure.

Put Secure Passwords to use.

A victim of cybercrime should notify the local cyber cell or a police station.

A complaint can also be submitted anonymously through the National Cybercrime Reporting Portal.

Conclusion

In conclusion, while a crime-free society is unachievable and simply a pipe dream, there should nonetheless be a constant endeavor to implement laws that keep criminality to a minimum. Legislators must go above and beyond to ward off impostors because criminality related to electronic law-breaking is bound to rise, especially in a world that depends more and more on technology. Technology is usually a two-edged sword that can be used for good as well as for bad intentions.

A number of laws have been passed by the legal system to address cybercrime against women. In order to ensure that technology advances in a healthy way and is used for legal and ethical economic growth rather than illegal activities, rulers and legislators should work continuously to achieve this.