Cybersecurity Concerns: Safeguarding Women and Children from Online Crimes

Authors:

Prof. Jharna Jagtiani, Assistant Professor, IFIM Law School, Bengaluru

Ms. Poorvi Gyanchandani, Student, IFIM Law School, Bengaluru

ABSTRACT

The Internet has evolved into a social and communication tool, with e-mails serving as an effective means of communication. The Internet provides new opportunities for networking and participatory democracy, and many young people are engaging socially through social media networks such as WhatsApp, Facebook, Twitter, and similar other platforms, becoming addicted to these Internet social activities and thus vulnerable to Internet crimes.

Individuals' and organisations' increased reliance on cyberspace has increased cybercrime. In India, we find that there is negligible proper training and education regarding such developments, and this ignorance has paved the way for cybercrime. Even the authorities and officers in charge of such cases lack the necessary training and expertise to commit cybercrimes against women, children, and girls in particular. The overall number of cybercrime occurrences increased by 18.4% in 2019, according to data from the National Crime Record Bureau, but the proportion of cases involving women increased by 28%.

The threatening environment created by such heinous cybercrimes against women and girls necessitates a radical shift in technology, behaviour, and legal affairs, which can be facilitated by proper education and training.

India should consider a proactive approach in which technology and a proper legislative framework work together to combat cybercrime.

This research paper attempts to investigate the problems and issues of cybercrime against women and children to present preventive strategies and means of retaliation with the help of cohesive forces.

Keywords
Cybercrime, cyberspace, women, children, Internet

Authors:
Prof. Jharna Jagtiani, Assistant Professor, IFIM Law School, Bengaluru
Ms. Poorvi Gyanchandani, Student, IFIM Law School, Bengaluru

INTRODUCTION

In old Indian culture, women are highly regarded. The Vedas celebrated women as the mother, the originator, and the one who gives birth, and revered them as "Devi" or "Goddesses."

Women are now viewed and portrayed as sex objects and treated as inferior to men in many cultural domains and functions, to the extent that even males believe their evil deeds against women cannot be punished. As a result, there is a sizable gender bias between men and women. Internet bullying and cybercrime are similar in that the perpetrators are not frightened of any authority that can punish them. In the virtual reality that exists in the online world, anyone can conceal or even pretend to be someone else. The criminal -minded exploit this gift of the internet to perpetrate wrongdoings and then conceal themselves behind the shield it offers. The essence of many technical advancements and advances is digital India. More than half of the population regularly uses computers, the internet, and other technology. The majority of these are social media sites, including Facebook, chat rooms, Instagram, Skype, WhatsApp, dating websites, etc.

The digitalization of the Indian system has enhanced every aspect, including governance, the economy, and education, but it has also drawn a sizable number of cyber criminals. Crime has been a social and economic phenomenon for as

long as there has been human civilization. A crime or offense is a legal wrong that may be the focus of criminal investigations and accompanying penalties. Depending on how it manifests, crime can have either direct or indirect effects on society. A wide variety of new offenses that have emerged as a result of the ongoing increase in the use of computers and the internet are referred to as "cyber crimes," which is a general term. Women in Indian society are the real targets of cybercrime. No definition is provided for the term "cybercrime," which is ambiguous because it can refer to any crime that is going to be committed using the internet or any other form of communication.

To understand the concept of cybercrime, one must first understand the concept of crime as it relates to computers and the internet. In many ways, the concept of cybercrime is similar to the concept of traditional crime. Both involve actions or inactions that result in a violation of the law and a response from the state.

Cybercrime is defined as those species whose genus is a conventional crime, regardless of whether the computer is the target of the crime or is used as a tool. The term "cybercrime" refers to any criminal activity that uses a computer, whether as a tool, a target, or a means of committing other crimes.

CYBER CRIME AGAINST WOMEN

Cybercrime targeting women is a common problem today. One Indian woman falls victim to cybercrimes every two seconds, and the internet world has emerged as the new stage on which a woman's security, privacy, and dignity are constantly threatened. Some criminals are using technology to vilify women by sending offensive emails, using WhatsApp, stalking them on websites and in chats, and,

worst of all, creating pornographic videos—the majority of which are done without the women's consent—by using online software to spoof emails and morph images for pornographic content.

Due to a lack of knowledge about appropriate reporting avenues or a desire to avoid the possibility of social embarrassment, Indian women are unable to immediately report cybercrimes. The primary objective of protecting women's safety is to prevent physical harm, but cybercrimes primarily affect them psychologically rather than physically. In this regard, it can be said that women's mindsets, in particular, need to broaden. Women must act as the whip to take out such criminals, such as by filing an immediate complaint and putting them in jail. Most of the problems can be solved if women report the crime immediately and warn the abuser about taking strong legal action.

In India, harassers and abusers are increasingly using online platforms to harass and mistreat women. Women are mostly targeted for cyberstalking, extortion, blackmail, etc. Women often trust criminals or abusers with their personal information, resulting in numerous cybercrimes. Many times, perpetrators get a chance to harass, abuse, and blackmail. The process for reporting a complaint is frequently unknown by women and children, giving offenders more chances to harass, abuse, extort, and so forth. Facebook, Twitter, and other social media sites seriously harm women because of the serious blackmailing, threatening, bullying, or cheating that takes place there via email and messenger. Theft of information, extortion, blackmail, sexual exploitation, defamation, taking control through pranks, retaliation, and insulting a woman's modesty are just a few of the male-committed cybercrimes.

SOME MAJOR CYBER CRIME AGAINST WOMEN

Thousands of women have been affected by conditions like depression and hypertension as a result of some of the most well-known major cybercrimes. In addition to anxiety, heart disease, diabetes, and thyroid issues, harassment also affects women negatively. Examples of notable cybercrime include the following:

Women are the most likely targets of cyberstalking, which is on the rise. Cyberstalking is a way to use the Internet to stalk someone for online harassment and abuse. Instead of directly threatening to hurt a victim physically, a cyberstalker will watch their online activity to get to know them better and intimidate them verbally.

BURNISHED LAW JOURNAL

Harassment through emails is not a new concept. It's a lot like harassing someone through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via email.

Libel and defamation both fall under the umbrella of "cyber defamation." It involves disseminating false information about the subject online or among the victim's or an organization's social and friend networks, which is a clear-cut way to ruin a woman's reputation by causing her excruciating mental anguish and pain.

Email spoofing generally refers to an email that emerges from one source but has been sent from another source. It can cause monetary damage.

Phishing is the process of trying to acquire sensitive information, such as a username and password, to obtain personal information.

Morphing is the process of changing an original image by an unauthorized user or while assuming a false identity. It was found that fake users had downloaded female pictures, edited them, and then created fake profiles before reposting or uploading them on different websites.

Trolls are criminals who post offensive or provocative comments in online communities to cause conflict or upsetting victims to elicit an emotional or disturbing response from them. Cyberpornography is another concern for female internet users. This would include technology-based websites and publications that are online and have explicit content.

BURNISHED LAW JOURNAL

CYBERCRIME AGAINST CHILDREN

Some of the most frequent crimes performed on digital platforms include cyberbullying, sextortion, cybersex trafficking, phishing emails, child pornography, sexually explicit content for children, sexual abuse, etc. Another demographic that is particularly vulnerable to these cybercrimes is children. The perpetrator can easily win the child's trust before enticing him or her because of the child's intelligence. Children who have been exposed to sexually explicit content online are more inclined to resort to the dark corners of the internet where they can more easily engage in sexual abuse. It is impossible to deny that children are sexually exploited.

THE MOST COMMON CYBERCRIME THAT AFFECT CHILDREN

According to Indian law, children are especially vulnerable to the most common forms of cybercrime, like cyberbullying and child grooming.

Cyberbullying is a form of bullying in which a child is repeatedly subjected to hurtful, cruel, and malicious remarks.

Children are particularly prone to these bullying actions because of their unstable emotional states. Another sort of crime against children committed through digital media is child grooming. Before luring a child into a sexual relationship, you must first establish a trustworthy and fiduciary relationship. By comprehending the mental capabilities of children, child groomers may manipulate and dominate them.

NCRB DATA

Children are particularly susceptible to the most prevalent types of cybercrime, such as cyberbullying and child grooming, according to Indian legislation.

According to Indian law, children are especially vulnerable to the most common forms of cybercrime, like cyberbullying and child grooming. Due to their unstable mental states, children are especially vulnerable to these bullying behaviours. This coarse and aggressive language seriously impairs the child's mental capabilities.

Child grooming is another type of crime against minors performed through digital media. Before attempting to lure a child into a sexual connection, one must first establish a trustworthy and fiduciary relationship with them. KVM Prasad, Assistant Commissioner of Police (Cyber Crime), Hyderabad, claims that because of increased public awareness of cybercrimes, more people are coming forward to report such incidents. According to him, the main reason for the rise in NCRB figures is that more people are reporting cybercrimes, even though the number of cybercrimes has somewhat increased. Three individuals are killed every hour, and a woman is hurt every 74 seconds. These are a few of the statistics from the NCRB[1]. Every 74 seconds on average, a crime against women was reported in 2021. Similar to this, 80 killings occur daily in India. These statistics were revealed in the 2021 "Crime in India" report released by the National Crime Records Bureau of the Union Home

Ministry (NCRB). Here are the key figures:

WOMEN

In India, there were 4,28,278 total cases of crimes against women in 2021, up 15% from the year before. Every 74 seconds on average in 2021, a case of a crime against a woman will be reported in India. Of these, "cruelty by husband" saw the largest number of cases—almost 32 per cent—followed by cases registered under

[1] As per NCRB (National Crime Records Bureau) data. A comparison for the year 2019 and 2021. It was observed majorly in cities like UP and other states.

'assault on women with intent to outrage her modesty' (20 per cent). In 2021, India reported 52,974 cybercrime cases, up more than 5% from 2020 (50,035 cases) and more than 15% from 2019. (44,735 cases).

Telangana, Uttar Pradesh, Karnataka, Maharashtra, and Assam were responsible for more than 70% of cybercrime incidents. The average number of cybercrime incidents per 100,000 people in the country was 3.9.

OFFENCES UNDER THE IT ACT 2000

The IT Act [2]tends to offences incorporating altering PC source archives, which incorporate-

Section 65 manages the hacking of PC framework.

Section 66 manages the distribution of data that is vulgar in electronic structure.

Section 67 manages Admittance to the safeguarded framework.

Section 70 manages Break of secrecy and protection.

REASONING BEHIND THE WRONGDOING

The explanations behind the rising cybercrime rate against women can be arranged into two classes: lawful and humanistic reasons. As this is extremely clear, the rule managing cybercrime doesn't explicitly cover those violations under the connected segments; then again, different regulations like the IPC, the Constitution, and so forth give exceptional security to ladies, yet similar insurance appears not to be given every day under the resolution. Normally, such victims accept that they are to blame for the wrongdoing committed against them.

BURNISHED LAW JOURNAL

THE INDIAN PENAL CODE 1860

Before 2013, no regulation managed cyberbullying or other violations committed against women on the web. Segments 354A to 354D are added to the Indian

Punitive Code, 1860, because of Area 354A of the 2013 Criminal Alteration Act.

Section 354A:

As per Segment 354A, a male who takes part in any of the accompanying demonstrations requesting or arguing for sexual blessings, showing porn against a lady's will; or offering sexual comments commits inappropriate behaviour and

[2] IT Act, 2000

might be rebuffed with thorough detention for as long as three years, a fine, or both. In the first two cases, it is possible to spend up to a year in jail, pay a fine, or do both.

Section 354C:

Voyeurism is characterized in Section 354C as the act of taking a picture of a lady taking part in a confidential demonstration or potentially distributing it without the woman's consent. For something to be considered "voyeurism," the circumstances must be such that the woman would "typically expect not to be seen, either by the wrongdoer or by any other person acting in the culprit's direction." If the defendant is found blameworthy under this segment, the guilty party might be fined and sentenced to as long as three years in jail on the principal conviction and seven years on the resulting conviction.

Section 354D:

The expansion of Segment 354D states about following disallowance, which covers the web-based following. When a man pursues or approaches a woman despite the woman's unmistakable lack of interest in the interaction, or when someone observes a woman's online behaviour, web usage, or electronic correspondence, this is characterized as a demonstration of following. Whenever viewed as being at real fault for following, a man could spend as long as three years in prison and a fine, and resulting convictions could land him in jail for as long as five years and a fine.

Notwithstanding the changes to the Code, various arrangements accommodate the detailing of digital assaults and the indictment of those who are capable.

Section 499:

To defame is to do something to hurt somebody's standing. When done with the intent to harm a lady's reputation, slander through the distribution of a moment and unambiguous depiction of attribution is punishable by up to two years in jail, a fine, or both.

Section 503: Criminal terrorizing occurs when an individual's reputation is harmed in order to drive her insane or force her to do something she normally does or does not do. This standard can be applied to circumstances where somebody is digitally coerced, as was done in the previously mentioned situation.

BURNISHED LAW JOURNAL

THE INFORMATION TECHNOLOGY ACT 2000

Section 66

Shankar v. State Rep[3]

The petitioner approached the Court under Section 482, CrPC to quash the charge sheet filed against him. The petitioner secured unauthorized access to the protected 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. The Court observed that the charge sheet filed against the petitioner cannot be quashed with respect to the law concerning non-granting of sanction of prosecution under Section 72 of the IT Act.

Section 66 A

Shreya Singhal V Union of India [3]

In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court. The Court noted that Section 66A of the IT Act is not violative of Article 14 of the Indian Constitution because there existed an intelligible difference between information communicated through the internet and other forms of speech. Also, the Apex Court did not even address the challenge of procedural unreasonableness because it is unconstitutional on substantive grounds.

Section 66C:

Fraud is a wrongdoing that is culpable under Segment 66C of the IT Act. This configuration would be appropriate in cases of digital hacking. According to this statement, anyone who erroneously or untrustworthy uses someone else's

[3] A. Shankar v. State Rep, Madras HC on 13th December 2010 Crl. O.P. No. 6628 of 2010 [3] Shreya Singhal v. Union of India, 2013 12 SCC 73

electronic mark, secret key, or other specific recognising highlight risks up to three years in jail and a fine of up to Rs. 1 lakh.

Section 67:

Revolting substances should not be distributed, communicated, or made to be conveyed under Segment 67, which conveys the most extreme sentence of three years' detention or a fine for a first conviction and as long as five years' detention and a fine for a second conviction.

Avnish Bajaj v. State (NCT) of Delhi[4]

The Court stated that Mr. Bajaj had no part in disseminating pornographic material. Additionally, the Bazee.com website did not allow access to the sexual content. However, Bazee.com makes money from the sales and from the adverts that are displayed on its website.

The Court further noted that the evidence gathered suggests that Bazee.com is not to blame for the cyber pornographic offence, but rather another individual. The Court granted Mr. Bajaj bail in exchange for the production of two sureties worth Rs. 1 lakh each. The onus is on the accused to prove that he was only a service provider and did not supply content.

BURNISHED LAW JOURNAL

[4] Avnish Bajaj v. State (NCT) of Delhi, 2008 150 DLT 769

INDECENT REPRESENTATION OF WOMEN BILL

Vulgar portrayals of ladies in distribution, promotion, and different media are precluded by this bill. With this section of the bill, the legal system will be expanded to include electronic and various media, as well as the dissemination of data on the internet and the portrayal of women on the internet. In any case, as of July 2021, this bill has been removed.

The 2013 Criminal Regulation Revision Mandate contains a few increments to the Indian Penal Code, like Sections 354 A, 354 B, 354 C, and 354 D. With the help of these segments, presently, the issues of MMS outrages, sexual entertainment, transformation, and criticism can be managed legitimately. As recently expressed, the supernatural idea of the Web is one of the essential purposes behind the development of cybercrime; In this way, while Section 75 of the IT Act manages offences or contradictions perpetrated externally in India, it doesn't address the locale of cybercrime, especially when the subject of the spot for detailing the case emerges when the wrongdoing is carried out in one area, impacted in another, and afterwards revealed in another. Nonetheless, the Criminal Methodology Code remains primarily concerned with regional jurisdiction.

Most cyber crimes stay unreported because of the reluctance and bashfulness of the person in question and her apprehension about maligning her family's name. The ladies are concerned that revealing the wrongdoing will make their lives more difficult; they are also concerned about whether their loved ones will support them and what society will think about them being aware of it. Because of these apprehensions, ladies frequently neglect to report their wrongdoings, making the spirits of the guilty parties get much higher.

WHY ARE CASES NOT BEING REGISTERED?

There's a significant distinction between a conventional examination and a digital examination, and to research cybercrime, a few specialized abilities are required. The police division is neither prepared nor equipped for digital and specialized examinations.

A large portion of the wrongdoing goes unreported because ladies have no clue about how to continue down the path of disgrace or dread. The pattern is currently changing as a direct result of better comprehension and mindfulness.

MEASURES TAKEN BY GOVERNMENT

As indicated by the Seventh Timetable of the Indian Constitution, "police" and "public request" are state subjects.

Through their Law Enforcement Agencies (LEAs), states and UTs are generally accountable for the counteraction, identification, examination, and indictment of wrongdoings, including cybercrime. Law Enforcement Agencies (LEAs), prosecute wrongdoers as per the law's arrangements.

Whereas the Central Government assists state governments in their capacity-building efforts by providing guidance and financial assistance through various programs.

A couple of drives taken by the focal government to advance the circumstance are referenced beneath.

CYBER CRIME PREVENTION AGAINST WOMEN & CHILDREN (CCPWC) SCHEME

Under the Cyber Crime Prevention for Women and Children (CCPWC) scheme, the Ministry of Home Affairs has provided financial assistance to all countries and UTs to strengthen the medium for dealing with cybercrime. The scheme is a hassle to assist countries in establishing cyber forensics training laboratories, training, and hiring inept cyber advisers. Under the action, cyber forensics and computer crime training laboratories have been established in 28 countries.

SPREADING AWARENESS ABOUT CYBER CRIMES

The development of cyber forensic technologies is one of the steps the central government has taken to raise public awareness of cybercrimes. Other steps include the release of alerts and advisories, capacity building and training for law enforcement, prosecutors, and judicial officials.

The Ministry of Electronics and Information Technology (MeitY) runs initiatives to increase awareness of information security. Children, parents, and general users can find information security-related books, films, and online resources.

INDIAN CYBER CRIME COORDINATION CENTER (ICCCC)

The government established the Indian Cyber Crime Coordination Center to provide a framework and ecosystem for LEAs to deal with cybercrimes thoroughly and systematically.

In order to address the issue of jurisdictional complexity, based on hotspots/areas for cybercrime, the ICCCC has established “Joint Cyber Coordination Teams” in Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Visakhapatnam, and Guwahati.

NATIONAL CYBERCRIME REPORTING PORTAL

To enable the public to report occurrences about all sorts of cybercrimes, with a focus on cybercrimes against women and children, the government has developed the National

Cyber Crime Reporting Portal

A module of the Citizen Financial Cyber Fraud Reporting and Management System has also been introduced to enable quick reporting of financial frauds and prevent money from being siphoned off by fraudsters.

OPINION

India and the USA, both these nations continue to use the same fundamental definition of cybercrime. An act, however, only qualifies as a criminal if the law so declares. Things start to become intriguing at this point.

IT-related rules are exceedingly rigorous and strictly enforced in the USA. However, IT-related legislation in India is poorly written, and enforcement is lax. A well-known instance would be piracy. In both jurisdictions, piracy is illegal. There is a good probability that one will receive some form of warning if they download something illegally in the US, either from the ISP or from police enforcement. There is an urgent need to aware society about the growing cyber crime in India on an individual basis and thereby make them aware of the measures and tools they have and can use against men or cyber crime criminals to secure themselves from being the ultimate victims of cyber crime. Our Indian Technology Act and IPC are still silent on some of the proactive measures that should be taken by women to free themselves from the unwanted trap of cybercrime. The same was said and observed by the National Commission for Women (NCW) which reported that experts from the cyber sector deliberated on strategies to repair gaps in the current grievance redressal system during its fifth legislative review consultation on cybercrime against women.

CONCLUSION

The methods used and the persistent nature of the offenders are the main problems with cybercrime. The police, the court system, and the investigation agencies must keep up with web-based application developments to quickly identify the real offender. The legal system and regulatory bodies must keep up with technological developments and prevent newer technologies from becoming tools of exploitation and harassment. Governments have the authority to pass laws that ensure the defence of human rights, especially those of women, both online and offline.

Legislation should inform and teach all groups how to use their rights to communication in addition to safeguarding users. People need to learn how to be cautious online and how to take legal action if their rights are violated. At the same time, they need to develop their offline and online smarts. A lot of the problems with fighting cybercrime that existed in the past, like evidence loss and the absence of a cyber army, have been resolved the credit of which goes to the Criminal Law Amendment Bill (2013). A few changes still need to be made, such as having judges that are tech-savvy.

Cybercrimes against women are still regarded lightly in India due to the general decline in respect for women in modern culture and the difficulty many people have accepting the idea that even sharing someone's photo online is illegal. Because they have no moral justification in society, cybercrimes like email spoofing and morphing receive low punishments. This brings us to the most important point, where society must advance, where people must respect others' rights, and where people must comprehend what constitutes a crime. So that they can speak out against it, it is crucial to enhance women's awareness of the need to exercise caution when using online resources and to get the right help if they are ever a victim of cybercrime. In India, there is a major need for knowledge and technical development to prevent harassment of women.