CHANAKYA LAW REVIEW (CLR)

Vol. III (Issue 02), JULY-DEC, 2022, pp.98-108

Cyber Crimes against Women and Prevention

Samridhi Goyal[162]

ABSTRACT

Over the previous two decades, information technology has broadened to become the axis of today's global and technological progress. The internet offers every user with all of the necessary information as well as the quickest communication and sharing tool, making it the most valuable source of data. With the multiple advancements of the internet, internet-related crime has spread its roots in all directions. Individuals are at tremendous risk from cyber-crime. Women are the soft targets of this new sort of crime, which is a global occurrence. In this article, I have examined that how women are targeted by cybercrime and online security flaws. Despite the fact that crime against women is on the rise in many areas, being a victim of cybercrime may be a particularly distressing experience for a woman. Especially in India, where women are marginalised in society and the law fails to recognise cybercrime. In this work, I intend to describe the numerous sorts of cybercrimes that can be perpetrated against women, as well as how they affect her. I have also gone through some of the legislation that protect women in such situations, such as the Information Technology Act (2000) and Indian Penal Code, 1860. To reach at the conclusion, I have analyzed a number of well-known Cases in cybercrime (e.g., the Ritu Kohli case). At the end of this paper, I have discussed the alternatives available to cybercrime victims as well as the reforms that the legal system will need to do in order to effectively combat cyber criminals' increasing spirits.

Keywords: Cyber Crime, Women, Information Technology, Prevention, Security

INTRODUCTION

A 21-year-old lady saw an image of her face digitally placed on the body of another woman posted on a social networking site in the Salem region of Tamil Nadu in June 2016. She informed her parents and identified the culprit. He allegedly modified her picture using a

[162] B.A. LL.B., (4th Year), Army Institute of Law, Mohali

mobile phone app, uploaded it to the site, and tagged her in the post after she had refused his marriage proposal. A complaint was filed with the Cyber Crime Cell by the woman's father. She discovered another distorted photograph linked to her social networking account a few days later, this time with her name and her father's phone number. The woman committed suicide on the same day. In her suicide note, she expressed her complete ignorance about the distorted images and her failure to convince anybody.[163]

With the increasing use of the internet in our daily lives and the progress of information technology, the vulnerability of computer and internet users has risen dramatically in today's cyberspace. Modern computers/computing devices have a phenomenally high technological capacity, which allows for both misuse and criminal activity. Unfortunately, many people are unaware of the dangers they are exposed to while surfing the internet, posting on social networking sites, or keeping data on their computers. Criminals exploit internet as a platform to engage in a variety of illicit operations against people.

Women's safety has always been a concern, particularly in a country like India, where the rate of crime against women is growing like a coconut tree. It used to be restricted to roadways or areas far from home. Earlier, the safest location for a woman to protect herself from being victimised was her home, but that is no longer the case. For them, home is becoming an equally unsafe place, prone to crime.

CYBER CRIMES AGAINST WOMEN IN INDIA

India is one of the few countries to have passed the Information Technology Act of 2000 to tackle cybercrime. A number of cybercrime offences are defined in the Information Technology Act of 2000. Among the many undesirable deliberate actions on the internet, online abuse is a worldwide potential problem that has impacted online users of all ages, resulting in harassment such as gender bullying, trolling, stalking, and other forms of harassment. [164]

MEANING OF CYBER CRIMES

In common parlance, cyber-crime is any illegal activity that uses a computer as its primary means of commission.[165] A person's repetitive, unsolicited, hostile behaviour through cyberspace with the goal to intimidate, humiliate, threaten, harass, or stalk someone else is

[163] HINDUSTAN TIMES, https://www.hindustantimes.com/india-news/salem-woman-ends-life-after-facing-sexual-harassment-on-facebook/story-zoBB2zQEsoenHHIWQv68gM.html.

[164] LIVE MINT, http://www.livemint.com/Politics/St93190XdGvpiclGWwnX0I/For-victims-of-cyber-stalking-justice-is-elusive.html.

[165] Dr. Monika Jain, Victimization of women beneath cyberspace in Indian Upbringing, Bharati Law Review, April-June 2017.

known as cyber harassment. In other words any harassment perpetrated through electronic media such as social networking sites, chat rooms, or e-mail is also illegal under Indian law.

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)."

On the internet, women are the most vulnerable and easy targets, making it simple to prey on the uninformed. People, particularly women, are most likely to be victimised via social networking platforms. Email harassment, cyber stalking, cyber pornography, obscenity, defamation, morphing, and email spoofing are the most common cyber-crimes against women.

TYPES OF CYBER CRIMES AGAINST WOMEN

1. **Cyber stalking**- Stalking means following someone with the goal of harassing or victimising them. It is defined as repetitive and unwanted harassing behaviour that is threatening and is purposely directed at a specific individual (the victim), and that would make a reasonable person worry for their own or their family's bodily harm or death. Cyber stalking is a digital version of physical stalking that takes place over the internet using information technology. Cyber stalking is the practice of following someone using the internet, e-mail, or chat rooms. The Wikipedia defines cyber stalking, where the Internet or other electronic means is used to stalk or harass an individual, a group of individuals, or an organization. It include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass.[166]

   Cyber stalking does not involve any physical contact yet stalking through the internet has found favour among the offenders for certain advantages available like, ease of communication access to personal information and anonymity.[167] There are three ways in which cyber-stalking is conducted:-

   i. **Stalking via e-mail** - Harassment via email is a type of harassment that includes blackmailing, threatening, and sending love letters under false names or sending embarrassing emails to one's inbox on a regular basis. It is generally perceived of as a

[166]WIKIPEDIA, https://en.wikipedia.org/wiki/Cyberstalking.
[167] S. K. Verma, Raman Mittal, Legal Dimension of Cyberspace, New Delhi (2004), Indian Law Institute.

sort of stalking in which one or more people send unwelcome and often threatening electronic messages to another person on a regular basis. There isn't always a precise definition of what a harassing message should look or sound like.

ii. **Stalking through internet**- This is the serious aspect of cyber stalking, in which the stalker follows the victim's online activities and publishes false information about her on the internet.

iii. **Stalking through computer**- The stalker is a technocrat in this guise, and he can take control of the victim's computer as soon as it starts up. The stalker obtains access to and control of the victim's computer address in this incident. This type of cyber stalking necessitates a high level of technical knowledge in order to gain access to the target's computer, and the victim's only alternative is to disconnect the computer and abandon current internet address.

2. **Cyber defamation**: Another widespread cybercrime against women is defamation. Females are targeted more than guys, despite the fact that it can happen to either gender. When someone uses a computer or the internet to publicly broadcast defamatory information about another person, or sends defamatory texts or emails about that person, this is known as cyber defamation. Someone, for example, posts defamatory information about someone on a website or sends defamatory e-mails to all of that person's friends or relatives. Hacking someone's id on Facebook, Google, or any other social networking or mailing website is the most common method. It can also be done by creating a false profile of a person that has all of that individual's personal information, which resembles to be a genuine one to others on any website.
3. **Cyber pornography**: Female internet users are also at risk from cyber pornography. This encompasses pornographic websites with adult photographs and videos, as well as their distribution. The internet has made it easier to carry out crimes such as pornography. Pornographic and offensive content is now found on roughly half of all websites. Female members of society are being threatened in the name of pornographic websites in order to gain sexual favours or exact retaliation. The most common of these offences is morphing images with naked photographs and uploading them to pornographic websites. Because of the ease with which these sites can be found and accessed, more serious cybercrime has occurred.
4. **Morphing**: Morphing is the process of an unauthorised user altering an original photograph. It is typically carried out by an unauthorised user or a person using a false identity who downloads and edits the victim's original photo before uploading it. It has

been proven that deceptive users are more likely to download and share edited female photographs. This crime is committed with the intent of blackmailing or defaming the victims online.

5. **Privacy infringement**: Privacy infringement generally means the violation of privacy of any individual. It means taking photographs, making videos, records, private pictures and publishing them or sending them electronically to anyone without the consent of the individual. Any violation of the privacy is punishable and legal action can be taken against of it.[168]
6. **Online Trolling**: Trolling is characterised as making provocative or off-topic comments to females in online communities such as newsgroups, blogs, and social media (twitter or facebook) with the intention of disturbing them emotionally. It is carried out by trolls, who are professional abusers who fabricate false identification cards and utilise them for this reason to create a cold war atmosphere.
7. **Voyeurism**: The cybercrime voyeurism is committed when any man watches or captures the image of a women engaged in a private act in circumstances where she have the belief of not being observed either by the perpetrator or any other person but those images used to be disseminated.[169]
8. **Cyber Bullying**: Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.[170] The main aim and objective behind such crime may be to defame the target out of anger, hatred or frustration or secondly when the perpetrator wants to make simple fun of his friends, classmates, juniors or unknown net friends.[171]

LEGAL REMEDIES AVAILABLE TO VICTIMS OF CYBER CRIMES

In order to ensure legal safety on the internet, the courts have played a critical role. The public must have faith and trust in the justice system. The court exists to serve society, and it will always be the backbone that allows a community to thrive and expand. A victim of cybercrime has the following legal alternatives:

1) SEXUAL HARASSMENT: SECTION 354A IPC, 1860

A man committing any of the following acts:

[168] Vartika Vasu, Krishnapriya.G, Cyber Crime Against Women: A Cyber Exploitation, Volume II Issue I.
[169] Ibid.
[170] Oxford Dictionary.
[171] Shobhna Jeet, Cyber crimes against women in India: Information Technology Act, 2000, (2012).

i. Physical contact and advances involving unwelcome and explicit sexual overtures; or
ii. A demand or request for sexual favors; or
iii. Showing pornography against the will of a woman; or
iv. Making sexually coloured remarks,

Shall be guilty of the offence of sexual harassment. The first three offences of sexual harassment bring a sentence of rigorous imprisonment for a period of up to three years, a fine, or both. The last offence of sexual harassment bears a penalty of either imprisonment for a term up to one year, a fine, or both.

STALKING: SECTION 354 D IPC, 1860

Stalking is defined as any man who:

i. follows a woman and contacts, or seeks to contact, her in order to encourage personal interaction despite her evident expression of disinterest; or
ii. monitors a woman's usage of the internet, e-mail, or any other kind of electronic communication.

And anyone who commits stalking is subject to a fine as well as a sentence of imprisonment of either description for a period up to three years if convicted on the first charge.[172]

2) VIOLATION OF BODY PRIVACY: SECTION 66E IT ACT, 2000

Capturing an image of a person's private body part is punished by up to three years in prison or a fine of not more than two lakh rupees, or both.[173]

3) SECTION 66D IT ACT, 2000

Any person who cheats by personation using any communication device or computer resource is subject to a sentence of imprisonment of up to three years and a fine of up to one lakh rupees, or both.

4) SECTION 66C IT ACT, 2000

Any individual who fraudulently uses another person's electronic identity, such as their signature or password, faces a sentence of imprisonment of up to three years and a fine of up to one lakh rupees, or both.

5) VOYEURISM: SECTION 354 IPC, 1860

Any man who watches or captures the image of a woman engaged in a private act in circumstances where she would normally expect not to be observed wither by the perpetrator or by any other person at the perpetrator's behest, or disseminates such image

[172] Indian Penal Code, 1860, §354 D.
[173] Information Technology Act, 2000, §66 E.

shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years,[174] and shall also be liable to fine, and shall be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but may extend to seven years, and shall also be liable to fine.[175]

In a case where the victim consents to the capture of the images or any act but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered as an offence under this section.[176]

6) **PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM: SECTION 67 IT ACT, 2000**

Whoever publishes, transmits, or causes to be published in electronic form any material that is lascivious or appeals to the prurient interest, or if its effect is such that it tends to deprave and corrupt persons who are likely, in light of all relevant circumstances, to read, see, or hear the matter contained or embodied in it, shall be punished on **first conviction** with **imprisonment** of either description for a term which may **extend to three years** and with **fine** which may **extend to five lakh rupees.**[177]

7) **MATERIAL CONTAINING SEXUALLY EXPLICIT ACT, ETC IN ELECTRONIC FORM: SECTION 67A IT ACT, 2000**

Anybody who publishes, transmits, or causes to be published or transmitted in the electronic form any content containing sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees.[178]

8) **SECTION 72 IT ACT, 2000**

Any person who illegally discloses any electronic information or other material containing personal information about another person without that person's agreement faces a sentence of imprisonment of up to three years or a fine of up to five lakh rupees, or both.

CASE LAWS ON CYBER CRIMES AGAINST WOMEN

Because women are uninformed of where to report such crimes and are hesitant to do so, the majority of cybercrimes go unreported. In the year 2000, the infamous Ritu Kohli case was reported as the first such cybercrime targeting women.

[174] Indian Penal Code, 1860, §354 C.
[175] Supra.
[176] Supra.
[177] Information Technology Act, 2000 §67.
[178] Information Technology Act, 2000, §67 A.

1. **RITU KOHLI CASE:** It was India's first reported internet sex crime. It was first reported in Delhi on Sunday, June 18, 2000. Manish Kathuria, a 30-year-old software engineer, was arrested by Delhi police officials from the Crime Branch for harassing a woman by messaging on the internet. Manish reportedly used to chat on website www.micr.com under the name of Mrs. Ritu Kohli. While chatting, he used profane language and gave her home phone number to continue the conversation. Mrs. Kohli began receiving inappropriate calls at her home as a result. Mrs. Kohli filed a complaint as a result of the disturbances, and after an investigation, the Delhi police identified the perpetrator and began criminal proceedings against him under section 67 of the IT Act and section 509 of the IPC for insulting Ritu Kohli's modesty.[179]
2. **STATE OF TAMIL NADU V. SUHAS KATTI:** This is a case involving the posting of obscene, libellous, and irritating messages in a Yahoo chat group concerning a divorcee woman. The accused forwarded emails to the victim through a fake email account he set up in her name. The woman was harassed online after the texts were posted, and she began receiving unpleasant phone calls in the notion that she was soliciting. As a result, she filed a case with the Egmore Court in February 2004. The culprit was tracked down and apprehended by the Chennai police cyber department based on the complaint. In addition, the accused was found guilty of violating sections 469/509 of the Indian Penal Code and section 67 of the Information Technology Act, 2000.[180]
3. **PURI CYBER PORNOGRAPHY CASE:** This was the state of Odisha's first cyber pornography conviction. To exact revenge on the complaint, Jayant Kumar Das, an RTI activist, constructed a false E-mail account and a bogus profile of the complainant's wife, Biswajit Patnaik, a journalist. He added nasty remarks and linked the bogus profile to an American porn website. On the porn page, he also disclosed the victim's phone number. After receiving obscene messages and phone calls, the journalist filed a FIR against Das at Puri's Baselisahi police station in July 2012. The inquiry was taken up by the Crime Branch's Cyber Cell in August 2012, and Das was arrested on September 18, 2012.The Puri Sub-Divisional Judicial Magistrate Court convicted RTI campaigner Das in a cyber-pornography case to 6 years imprisonment under section 66C/67/67A of the Information Technology Act.

[179] Vishi Aggarwal & Ms. Shruti, Cybercrime victims: A comprehensive study,6, IJCRT, 646, 2018.
[180] INDIAN KANOON, State of Tamil Nadu v Suhas Katti – Cyber law case in India, indiankanoon.org.

4. **DR. PRAKASH V. STATE OF TAMIL NADU:**[181] In the state of Tamil Nadu, this is the first case to be prosecuted under the IT Act. The case involves sex, pornography, the internet, and a mastermind who is reportedly a medical doctor. Doctor was charged with manufacturing pornographic images and recordings of various acts of sexual intercourse and selling them to 23 nations, ruining the lives of many young girls who were subsequently detained. When Ganesh filed a complaint with the municipal police, claiming to be a victim of the doctor, the story came to light. A case was lodged against the doctor and he was booked under section 67 of the IT Act, which deals with obscenity, the sentence can be of 5 years imprisonment with a fine of Rs. 1000 on the first conviction and penalty may extend up to 10 years imprisonment with a fine of Rs. 2 lakhs on the second conviction.[182]

PREVENTION OF CYBER CRIMES AGAINST WOMEN

Ms. Maneka Gandhi, the Union Minister for Women and Child Development, stated in May 2016 that online harassment of women in India should be treated the same as physical violence against women, and she established a new venue for redress. She also asked the National Commission on Women to set up a strategy to address women's online abuse.[183]

The Information Technology Act of 2000, as well as the Indian Penal Code of 1860, have suitable cyber-crime prohibitions. The government has implemented a number of legislative, technical, and administrative steps to prevent and combat cybercrime. These inter-alia includes:-

a) Each state has established Cyber Police Stations and Cyber Crime Cells for the reporting and investigation of cyber-crime cases.
b) The Ministry of Electronics and Information Technology (MeitY) has established Cyber Forensics Training Labs in north-eastern states and cities such as Mumbai, Pune, Kolkata, and Bangalore to train state police officials and the judiciary in cybercrime detection, collection, preservation, and seizure of electronic evidence, and dealing with cybercrime. Various national and state police academies/judicial academies and other institutes have been established by the Ministry of Home Affairs, Meity, and State Governments to modernise the setup and equip police personnel with knowledge and skills for the prevention and control of cybercrime.

[181] AIR 2002 SC 3533.
[182] THE HINDU, www.thehindu.com.
[183] Online trolling against Women to be considered violence: Maneka Gandhi, Deccan Chronicle, 18th May'2016.

c) On June 6, 2016, the Ministry of Electronics and Information Technology published an advice on the operation of matrimonial websites under the Information Technology Act, 2000. There are additional rules instructing matrimonial websites to implement measures to guarantee that people using these services are not fooled by fraudulent profiles or the misuse/posting of incorrect information on their websites.
d) The government has issued and distributed a Computer Security Policy and Guidelines to all Ministries/Departments on how to avoid, detect, and mitigate cyber-attacks.
e) The Ministry of Home Affairs has created a website, www.cybercrime.gov.in, for the public to report cybercrime complaints.[184]

Even now, the Indian police appear to be unconcerned about cybercrime. In such cases, a woman or young girl who has been a victim of cybercrime should first contact a women's assistance cell or non-governmental organisation (such as the All India Women's Conference[185], Sakshi[186], Navjyoti[187], or the Centre for Cyber Victims Counseling[188]), which will assist and guide them through the process. This will also ensure that the police do not dismiss the case.

It is worth emphasising that women may have a role in controlling cyber obscenity by becoming aware of their rights and following the safety procedures in place. Some well-known social media companies provide a number of privacy settings to defend and protect women against predators. Keep in mind, however, that most well-known websites indicate in their privacy policies that they will not be held liable for any form of harassment perpetrated against users by other users.

Women should read the privacy regulations or safety measures connected to such offences before registering on any other social media network. In most situations, negligence and lack of vigilance are also contributing factors to women becoming targets of cyber obscenity.

CONCLUSION

According to the official statistics provided by the National Crime Records Bureau, Government of India 9622 cases of cyber-crimes were registered in 2014 and 5752 persons

[184] Abhinav Sharma & Ajay Singh, Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement 3 (2018), Volume 1 Issue 3.
[185] http://www.aiwc.org.in/ (Private group of women assisting other less fortunate women to fight the crimes committed against them).
[186] http://www.sakshingo.org/ (NGO assists women in dealing with govt. authorities).
[187] http://www.navjyoti.org.in/ (NGO by Kiran Bedi, assist women in several aspects).
[188] http://www.cybervictims.org/ (Private group of legal minded individuals who help the victims of cybercrimes).

arrested. In 2015, 11,592 cases were registered an increase of 20% in registration of cases from the previous year – and 8121 persons arrested. 4242 cases of cyber-crimes were registered in 2017.[189]

It is evident that cyber-crime against women has increased in our society with the arrival of information and technology, as well as access to the internet in nearly every hand. And it's past time for the legislative and the executive to work together to put a stop to it. Some of the prominent reasons for the growth of cyber-crimes against women can be regarded as:

- A large number of vulnerable targets- Loneliness is a major factor, as many female students and employees are separated from their families and work long hours at computers. As a result, the computers have become their trusted companion.
- Anonymity allows for easy concealment.
- Most cyber-crimes go unreported owing to fear of repercussions from society, reluctance, shyness, and the fear of defamation.[190]

To stay one step ahead of such criminals, the judiciary, as well as the police department and investigative agencies, should be equipped with current web-based technologies. The legal system and regulatory bodies have a responsibility to keep up with technology advancements and guarantee that emerging technologies do not become tools of exploitation and harassment. Though there were previously various challenges in dealing with cybercrime, such as the loss of evidence and the lack of a cyber-army, the Criminal Law Amendment Bill (2013) addressed the majority of these issues. Several adjustments, such as cyber-savvy judges, are still required. It can be stated that proper implementation of laws along with public awareness and education of women concerning their rights and legal remedies can play a crucial role in eradicating cybercrimes from our society.[191]

****

[189] Crime in India 2017, Ministry of Home Affairs, Government of India, https://ncrb.gov.in/en/cyber-crimes-statesuts.

[190] Abhinav Sharma & Ajay Singh, Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement 3 (2018), Volume 1 Issue 3.

[191] *Id.*