WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Crime against Women

Adil Abbas

Chanakya National Law University

ABSTRACT

One of the oldest civilizations in the world is that of India. In our country, women receive special care. They were held in high esteem, treated like goddesses. These fundamental rights have, however, been violated as society has modernised. India's information technology industry is growing quickly. The majority of daily tasks are performed by people using computers. It was thought that 2000 would be a transformative year for technology. Cybercrime is on the rise as more people use computers on a daily basis. In our country, women are also the most frequent victims of cybercrime. A new kind of crime has emerged: cybercrime. Online stalking, morphing, and cyber defamation are just a few examples of the varied forms that cybercrime can take. Women are being harassed via emails. People experience harassment, which is a pretty common occurrence in the modern world. Although the Information and Technology Act of 20001 was passed to fight against such crimes, it is ineffectual unless people change the way they think.

INTRODUCTION

India is progressing more quickly, and one of the major factors boosting its prosperity is technological innovation. It is important to note that humanity gains a great deal from revolutions. India is clearly developing in the area of technology, particularly information technology, at a rate that is unmatched. The idea of a modern India has placed a lot of focus on scientific infrastructure for its inclusive prosperity. Any forms of criminal activity that involve the use of technology—including computers, the internet, and cyberspace—to carry out unlawful acts are collectively referred to as cybercrime. Cybercrimes against women may take the form of stalking, extortion, defamation, harassment via emails, morphing photos, texts, etc. Fraudulent identification documents made on social networking platforms are typically used in cybercrimes against women.

In this, I'll talk about the different kinds of cybercrimes that are committed against women, their rising prevalence in 2018–19, and the role that the cyber department plays in handling these instances. Also, I will discuss several laws that exist to defend women from cybercrime, including the Technology Act and the IPC with its numerous case laws.

CYBERCRIME INCREASE STATISTICS

Cybercrimes are growing more quickly these days. The same has been illustrated with data from 2012 to 2020[2]:

Year	Number of cyber crimes
2012	2876
2013	4356
2014	9622
2015	11592
2016	12317
2017	21796
2018	27248
2019	44546
2020	50035

A total of 50,035 cases were reported in 2020, up from 44,546 the year before. Due to the global shutdown, more people chose to work or study from home while using digital devices. According to the National Council for Women, they received a total of 412 complaints regarding cyberbullying between

[1] Information Technology Act, 2000,No.21, Acts of Parliament, 2000 (India).

[2] NCRB, https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents (last visited March. 8, 2023).

March 25 and April 25, of which 396 were of a serious kind (including indecent exposure, unsolicited pornographic pictures, blackmail, threats, and ransom demands).[3]

Compared to the 12,092 offences against women that were filed in Delhi in 2019, there were 9,782 recorded offences against women in 2020. In other parts of India, there was a 21% drop in crime against women. A total of 35,331 occurrences of crime against women were recorded in 2020, as opposed to 44,738 incidents that were all reported in 2019.

Street crime significantly decreased as a result of lockdown. The installation of preventative measures, such as nighttime patrols and 24-hour street policing, was one of the factors that contributed to this alarming trend. Patrolling and checking were intensified at night.

Several Indian states experienced cybercrime in the year 2019:

State	Number of cybercrime Reported
Karnataka	12,007
UP	9,353
Assam	1,989
Telangana	1,629
Maharashtra	4,967

Hyderabad has reported 1,300 incidents during lockdown, and by 2020, there would be a 70% surge in cybercrimes in the city.[4] Additionally, the city with the highest recorded rate of cybercrime in CVID-19 is the IT powerhouse of Bangalore in Karnataka. Cybercrime increased by 40% in Maharashtra over the previous year. The nation's Technology capital is one of the areas that is most badly affected by cybercrime, according to studies.[5]

Reasons for the Growth of Cybercrime during Covid-19

First off, when there is a lockdown and individuals are heavily utilising their digital devices compared to other days, it is the simplest time to do cybercrime. It is thought that individuals who are knowledgeable about digital systems but who are unable to find employment or who have had their services terminated are more likely to engage in unlawful activity.

Throughout the pandemic, criminals used a variety of tactics to perform cybercrimes, including phoning victims and asking for their bank information while claiming to have won the lottery and having the money sent right to their bank accounts. There was a plot going on during lockdown where women were receiving emails alleging that their phones had been compromised and that Blackmailer would send their intimate photographs along with all of their contacts if they didn't put money into their accounts.

The founder of the Cyber Peace Foundation also asserts that "sextrotion" has increased during lockdown since more people are beginning relationships online while they are in lockdown. Threatening to disclose intimate photos of the victim or any other sexual information about them is known as sextrotion, which involves coercing someone into acting in a certain way, most often sexually. There have also been reports of women being deceived online, as soon as they click on fraudulent links that collect all of their private sensitive data on their smartphone, switch on the camera, and film their private moments, and these photographs are then used to blackmail them.

In one instance, cybercriminals send people targeted emails with a Covid-19 theme while posing as government representatives in order to obtain their personal information, such as home addresses, cell phone numbers, etc.[6]

A hospital has been the target of a cyber-attack where crucial files are being taken and held hostage until a ransom is paid. The World Health Organization (WHO) has also been the target of cyberattacks where employees' login information was taken. In one of the situations, an Indore-based Merchant Navy officer was requested to pay 62 lakh as processing fees after receiving an email about a refund of his customs duty. He paid up front but was not given a refund.

Throughout COVID-19, Cyber Peace has been receiving complaints from a variety of sources, and it has been noted that many are hesitant to file complaints. People believe that transactions in internet are informal. Since they worry about the resulting social disgrace, women are hesitant to voice their concerns. However, the mentioned official figure is just the beginning.[7]

[3] Available at: https://timesofindia.indiatimes.com/city/delhi/covid-effect-heinous-crimes-dip-cyber-fraud-up/articleshow/86243735.cms(last visited on March 8, 2023.

[4] Varun Wahane , The rise of cybercrimes in covid-19 pandemic ,IPLEADERS (Sep.9,2022, 3:34 PM),https://blog.ipleaders.in/rise-cybercrimes-covid-19-lockdown/

[5] Id. at 12.

[6] The Indian Penal Code ,Supra note 5, at 2.

[7] NDTV, https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-duringlockdown-experts-222235 (last visited March. 8, 2023)

Three people were detained in Bengaluru on suspicion of participating in sextortion and other forms of cyber fraud; nationwide, approximately 4,000 cases of this nature have been lodged[8]. A person who had improperly obtained adhaar information to apply for loans was detained by the cybercrime police team in Kolkata (through mobile banking applications)[9]

Legal Remedies available to a Victim of Cyber Crime

The Indian government has recognised several different types of cybercrimes. The following list of crimes and their remedies is provided:

1. **Cyber pornography or publishing any obscene sexual material**- when any pornographic content is published, produced, transferred, or distributed via the internet. Obscene material is defined as "material that is punishable with imprisonment for up to two years or a fine of Rs. 2000 or both" in Section 292 of the IPC, 1860. In addition, Section 67 of the IT Act specified that "obscene material is punishable with imprisonment up to three years and a fine of Rs 500."[10]
2. **Cyber blackmailing/cyber stalking**- According to the NCRB report, 58% of women reported experiencing cyberbullying, which includes harassment by email and text message and is illegal under Section 67 of the IT Act and is punishable by up to five years in prison. Cyberbullying is the act of posting sensitive information about someone with the goal to torment them using the internet or any other digital transmission method.
3. **Cyber blackmailing** – The act of threatening to divulge or publishing personal information about a specific individual in return for monetary, sexual, or other demands is referred to as this practise. Extortion is defined by Sections 384 and 385 of the IPC, 1860, and is punishable by up to three years in prison, a fine, or both.
4. **Cyber stalking**- It is the bothersome practise of contacting someone online or learning more about them online. It is a violation of the IPC's Section 354D, which carries a fine and a sentence of up to three years in prison.[11]
5. **Defamation**- It is the act of sullying someone's reputation by stating or publishing false information about them. According to sections 499 and 500 of the IPC, defamation is defined as an act that is punishable by up to two years in prison, a fine, or both.[12]

Judicial View on the Issue

In Suhas Katti v. State of Tamil Nadu[13], one of the most significant cyberpornography cases in India, the court sentenced the accused under Sections 67 of the Information Technology Act and Sections 509 and 469 of the Indian Penal Code, 1860, for posting obscene material by harming the reputation and character of the women. This was the country's first conviction for online pornography.

Also, the perpetrator and victim in State of West Bengal v. Animesh Boxi, (instance of revenge porn), were partners at the time the perpetrator received some of the victim's intimate photos. Later, in an effort to exact revenge, he started using them to blackmail her and posting them online. Articles 66E, 66C, 67, and 67A of the IT Act of 2000, as well as Sections 354A, 354C, and 509 of the IPC of 1860, were used to prosecute the offender in this instance.

According to Shreya Singh[14] Section 66 of the Act, anyone who sends or receives content that is offensive, false, or likely to cause annoyance, discomfort, danger, insult, hate, hurt, or ill will is punished. was overturned due to its vagueness and application of the chilling effect doctrine. The court held that merely advocating for a cause, regardless of how unpopular, falls within the scope of the fundamental right to free speech and expression and is ineligible for a defence under Article 19(2), and that section 66A's restrictions on all forms of communication were unreasonable and unjustified.

Shamsher Singh[15] After the High Court denied the plea to show the compact disc presented in defence and have it proven by the forensic science laboratory, the accused filed an appeal with the Supreme Court. The Supreme Court determined that compact discs are very well a document for the purposes of section 294(1) of the Criminal Procedure Code[16] and as such, it is not necessary to obtain personal permission for admission or denial from complainant, accused, or witness.

CRITICAL ANALYSIS

States typically have major problems with the rise in crimes against women, but the issue is exacerbated by cybercrime because of the possibility of criminals using several identities. Since "Internet Service Providers (ISP)" are the only ones who have a complete record of all the data that everyone

[8] Id. at 23.
[9] Id. at 23.
[10] Information Technology Act, 2000, S 67, No.21, Acts of Parliament, 2000 (India)
[11] The Indian Penal Code, 1860, S 384, No.45, Acts of Parliament, 1860 (India)
[12] The Indian Penal Code, 1860, S 499, No.45, Acts of Parliament, 1860 (India).
[13] Order passed on 5th November 2014 in CC NO 4680 of 2014
[14] Shamsher Singh Verma v. State of Haryana 2015 SCC Online SC 1242.
[15] Shreya Singhal v. Union of India (2013) 12 SCC 73
[16] The Code of Criminal Procedure, 1973,No.02, Acts of Parliament, 1974 (India)

with internet access may access, the government should place strict laws on them to combat this. ISPs should be required to notify authorities of any questionable activity by any user; doing so will assist prevent crimes from occurring in the first place. Lawmakers should impose stricter regulations on internet cafes that require them to keep accurate, complete records of the customers who use their services. Cybercafés are frequently used by criminals to conceal their IP addresses from investigators in the future. Another method of obscuring one's identity is this. People should be aware of the extent to which their daily lives are being recorded on camera and should react appropriately when this occurs. Also, it's critical to spread knowledge of digital places and their effects. It's crucial to inform individuals of their rights. Surveys reveal that the vast majority of internet users in India are unaware of their rights in these areas.

Only Section 292 of the IPC makes it criminal to publish, impart, or influence someone to publish information in electronic form if it can be demonstrated that this has happened. Other cybercrimes included by the Technology Act of 2000 include email spoofing, morphing, and cyberstalking. Indian women who use the internet are hesitant to report cybercrimes out of concern for being identified in public. Even if these occurrences are happening more frequently, relatively few victims are prepared to come forward and ask for justice.

PRECAUTIONS/SUGGESTIONS/CONCLUSION

1. The only company with a thorough record of all the data viewed by everyone experiencing internet issues is the ISP. As a result, "Internet Service Providers" should be subject to strict controls from the government.
2. People must be made aware of their rights and of cyberlaws. According to a study, a significant portion of Indian citizens are unaware of their rights.
3. Approach the police when you are a victim of cybercrime.
4. Need to make strict regulation for cyber cafes.
5. Do not share personal information and photos on social media as it’s not secure.

REFERENCE

1. Information Technology Act, 2000,No.21, Acts of Parliament, 2000 (India)
2. The Indian Penal Code, 1860,No.45, Acts of Parliament, 1860 (India).
3. Saumya Tripathi, Reason for the growth of cyber crime in india, Lawsisto (Sep. 8, 2022**)** https://lawsisto.com/legalnewsread/NjY5NA==/REASONS-FOR-THE- GROWTH-OF-CYBER-CRIME-IN-INDIA/
4. The Indian Penal Code, 1860, S 292, No.45, Acts of Parliament, 1860 (India).
5. Information Technology Act, 2000, S 67, No.21, Acts of Parliament, 2000 (India).
6. Information Technology Act, 2000, S 7, No.21, Acts of Parliament, 2000 (India).
7. The Code of Criminal Procedure, 1973,No.02, Acts of Parliament, 1974 (India)