ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 12, December 2021 SJIF 2021 = 7.492
A peer reviewed journal

A REVIEW ON CYBERCRIMES AGAINST THE WOMEN

Pradeep Kashyap*

*Lecturer,
Department of Business Law, Faculty of Commerce, Management & law,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: pradipprgnul@gmail.com

DOI: 10.5958/2249-7137.2021.02678.1

ABSTRACT

Inventions have always been a component of society's evolution. The internet has been a benefit to society since its beginnings, but with the passage of time and continued usage, it has also resulted in some disadvantages. On the one hand, internet use has a beneficial effect, but it has also provided a route for serious cyber-crime in recent years. In this article, we will concentrate on cybercrimes affecting women across the world, such as stalking, unethical hacking, cyber bullying, and forced pornography viewing. Women's crime is one of the most common types of crime, and it is growing at an alarming pace across the world. Women's crime is on the rise, and this includes violence against women in the digital age. In an age of technology when young people are more exposed to it, crime rates in the virtual world are rising at a similar pace. People in India are mostly unaware about cybercrime. Cybercrime may take various forms. In this article, we primarily focus on cybercrime in India. Women in India have always been looked down upon, and there have never been any laws in place to protect them. We have examined and offered potential recommendations in this article as to what should be depended on and what adjustments should be done in the legal system to effectively control the growing spirit of cyber criminals.

KEYWORDS: *Cyber Stalking, Cybercriminals, Defamatory, Scandal, VAWG Strategies, Unethical Hacking.*

1. INTRODUCTION

The cyber world, which we call the virtual world because it is an extension of the actual world, has crimes that include the use of technology, and such crimes are referred to as cybercrimes because they involve the use of technology, particularly computers and the internet. Individuals, businesses, and even the government are all targets of cybercrime. Such crimes are not committed by a physical entity; rather, they are assaults on information accessible on the internet, i.e. on a person's or company's virtual body[1].

Cybercrime is on the rise, as internet access has been made accessible to even children who have no understanding of the benefits and drawbacks of using the internet. Even children are now exposed to the usage of the internet, as a result of the current pandemic scenario, education has been fully digitalized, and such exposures are proving to be detrimental, as pupils at a young age

are exposed to platforms other than instructional software. As a consequence, there will be taps, as well as more sextortion and cyberbullying[2].

The easy accessibility of the internet, the rapid spread of mobile information, and the widespread use of social media, combined with the current situation of violence against women, has resulted in the emergence of a cyber Violence Against Women and Girls (VAWG) strategy as a growing global problem with potentially significant economic and societal implications. The VAWG approach is a funded program that assists victims, tries to prevent others from becoming victims, and seeks to bring justice to the victims. Despite the relatively new and increasing phenomena of global connection, every other woman will suffer some kind of violence in her lifetime. At the age of 15, one out of every 10 women has already suffered some kind of online abuse. Internet access is becoming a requirement for economic well-being and aids in the country's economic growth[3].

It is critical to ensure that this digital public space is secure and that everyone, especially women and girls, has access to it. Cyber stalking, non-consensual pornography (or revenge porn), gender-based insults and harassment, unsolicited pornography, extortion rape and murder threats, and electronically facilitated trafficking are all examples of cyber VAWG. The possibility of cyber-violence manifesting psychically should likewise not be overlooked. To further understand the effect of cyber VAWG, more study into victims' experiences is required.

2. DISCUSSION

2.1 Stalking on the Internet:

Cyber stalking is the practice of using the internet to contact or track the activities of strangers through email, text, or online communications, or via social media. Internet stalking entails a series of events that may or may not be benign in and of itself, but when taken together, threaten the victim's feeling of safety and create anxiety, worry, or panic. Cyber stalking is a criminal offense since it causes harassment, defamation, slander, and intimidation of the victim.

The Indian Penal Code, Indian Penal Code (Amendment) Act, 2013, and the Information Technology Act, 2000 make cyber stalking illegal and punishable. According to Section 354D of the Indian Penal Code (Amendment) Act, 2013, cyber stalking is defined as "following or attempting to contact a person repeatedly, despite the other person's disinterest," and "trying to harass the person by using the internet and various other online resources or platforms and causing disturbance to the victim's mental health."

Sections 499, 354A, 354C, 503, 509 of the Indian Penal Code, 1860, deal with defamation, punishment for sexual harassment, punishment for capturing images of women engaged in private activities without their consent, punishment for criminal intimidation, i.e. threatening to cause injury to a person's reputation, and punishment for outraging the modesty of a woman.

The Information Technology Act of 2000, Sections 66E, 67, 67A, and 67B, emphasize problems and legislative measures relating to cyber stalking and other cyber offenses. Cyberstalking is addressed under Section 72 of the Information Technology Act of 2008[4].

The Ritu Kohli Instance was India's first recorded case of cyber stalking, in which Mrs. Ritu Kohli complained to authorities in Delhi about a person who was using her identity to communicate over the Internet for a continuous period of four days. Mrs. Kohli went on to say

that the individual was speaking with her, using her name and address, and using filthy language. The same individual also gave her contact information through chat, resulting in her receiving calls at strange hours. She got almost 40 phone calls before filing another complaint, which resulted in the IP address being tracked and the perpetrator being apprehended. Following that, a case was filed against him under section 509 of the Indian Penal Code, 1860, and he was freed on bail.

2.2 Acts may include the following:

Sending abusive or threatening emails, text messages (SMS), or instant communications: Videotaping someone without their permission and then posting or utilizing such recordings to blackmail them. Hacking of social media accounts, as well as tampering with photos and personal information[5].

Making derogatory remarks about the victim on the internet, cyber-assault, and threats of rape on social media are all examples of cyber-assault. A cybercrime was reported in Sweden, where the raped victim was broadcast online using the 'Facebook live' function8. Sharing the victim's private pictures or videos on the internet or through mobile phone.

2.3 Harassment on the Internet:

Cyber harassment, also known as cyber-bullying, is an unethical act of intruding into an individual's personal space via online tools, such as accessing someone's e-mail ID without their consent, unethical hacking, posting defamatory statements or sharing obscene images on social media accounts, threatening someone via threat messages sent over the internet, and so on[6].

Cyber harassment may take many different forms, however for the purposes of this article, it can involve the following:

- Unwanted sexually explicit emails, SMS messages (or online)
- Hate speech, which is defined as language that denigrates, degrades, threatens, or attacks a person based on her identity (gender and other characteristics); • Offensive or improper approaches on social networking websites or online chat rooms; (such as sexual orientation or disability)
- Hacking into someone's internet accounts and distributing obscene pictures with the intent to exploit them are examples of cyber-harassment.
- Sextortion, in which women are enticed to deposit money into cyber criminals' accounts through phishing e-mails, or they are warned that their pictures would be stolen from social media accounts and edited into filthy images. This method is used to blackmail women in order to get money from them.

In 2004, a DPS (Delhi Public School) student used his mobile phone to record a sexually explicit video clip of a classmate in a compromising situation and sent it to his pals through MMS. The video was subsequently uploaded on Bazee.com and extensively shared. Tamil Nadu is a state in India. V. Suhas Katti is noteworthy for obtaining a successful conviction in a very short period of time, just 7 months after the FIR was filed[7]. A case involving the publication of an obscene, defamatory, and irritating comment in a Yahoo chat group concerning a divorcee lady. On

November 5, 2004, the Additional Chief Metropolitan Magistrate issued the following judgment: The defendant has been found guilty.

2.4 Pornography that is not consented to:

Non-consensual pornography, often known as cyber exploitation or "revenge porn," is the online sharing of sexually explicit pictures or video without the permission of the person shown. In most cases, the offender is an ex-partner who gets images or videos from a previous relationship in order to publicly humiliate and disgrace the victim in retribution for terminating the relationship. However, offenders aren't usually partners or ex-lovers, and vengeance isn't always the motivation. Images may also be acquired via breaking into a victim's computer, social media accounts, or phone, and can be used to cause real-world harm to the target (such as getting them fired from their job)[1].

2.5 MMS Scandal in Noida:

In February 2009, an MBA student in Noida used his girlfriend's e-mail address to send a video clip of his 23-year-old girlfriend stripping for him to his classmates.

When the girl declined to marry him, the boy with access to the girl's email id shared the MMS footage with his classmates[8].

Following a complaint from the girl's family, police opened a criminal intimidation investigation in order to protect women both online and offline.

1. Police reactions should recognize that cyber VAWG is a kind of VAWG. STRATEGIES for combating cyber VAWG must also incorporate the voices of women who have been victims of the phenomena.
2. The definition of cybercrime on the migration and affairs website should be amended as soon as possible to include a form of cyber VAWG, or at the very least, misogyny in the third party of its description.
3. The general people should be better knowledgeable about cyber legislation.
4. There should be more appropriate legislative provisions in place to keep track of internet use. Convicting cybercriminals is essential for effective legal enforcement of cyber laws because they can jeopardize a user's reputation, finances, physical integrity, data, and privacy, as well as because cybercrime has economic consequences and indirectly promotes traditional violent crimes, terrorism, and money laundering schemes. Spreading awareness of good internet practices such as installing antivirus, firewalls, practicing safe shopping and clicking, avoiding the disclosure of sensitive information, system updating, and using strong passwords can help to reduce the number of cybercrimes and even add evidence to help convict cybercriminals[2].

People must also be informed of the law enforcement procedures and infrastructure in place in their nations in order to report cybercrime and prosecute instances successfully. Few people in India are aware of the Adjudication Authority, which is authorized under the IT Act of 2000 to hear instances of cyber-violations and issue decisions imposing penalties in the form of damages and compensation. Better awareness may be disseminated through offering specialized licensed courses, hosting seminars and workshops, using print and electronic media, mass campaigns, and

enlisting the help of industry experts, cyber attorneys, and forensic organizations, among other methods. International Organizations should participate in seminars and workshops led by members of the judiciary, police and legal experts, and industry associations, so that cyber laws can be discussed from a global perspective and policymakers can learn about new technical, policy, and legal measures (substantive and procedural) being implemented in other jurisdictions to harmonize cyber laws and their enforcement[9].

2.6 Cyber Crime During Covid-19:

As we all know, is a pandemic that has had an effect all over the world and has impacted everyone's daily lives. During the pandemic, we encountered many difficulties in our daily lives; similarly, mafias in the cyber realm took advantage of this moment to create evil out of good.

This epidemic has provided chances for incarcerated criminals to target a certain segment of society (mostly women) and harass them online.

The National Commission for Women (NCW) in Delhi has submitted a report to a daily newspaper stating that the number of instances of cyber-crimes against women has risen dramatically since the countrywide lockdown was imposed. Women have been targeted by the imprisoned cyber criminals, who have been sending them constant threat e-mails with threats of sextortion using altered pictures to collect money from them. Phishing e-mails and increasing dependence on information accessible on the social networking site were also used to target women[10].

3. CONCLUSION

With the rise of Covid-19 in the recent times, and even before these cyber-crimes against women had been a worldwide issue and a major area of concern. Going with the recent statistics, the crimes in the cyber space has drastically increased by 86%17. Cybercrimes have become an increasing threat to the individuals, especially women, as they are treated vulnerably in India. In the technologically advanced time, our personal data stored in the software or otherwise are at high risk. Taking into account the above-mentioned scenario, we, in this paper propose few possible suggestions which might help in reducing the number of victims who are victimized by cyber criminals. The following are the proposed ways which can be taken into consideration:

With changing time technology is updating, therefore to keep our data safe and secure we need to keep our data protected by using password as well as other protection such as fingerprint recognition, eye retina scanner etc. Proper awareness programs must be organized to make people aware of how to identify that a particular material over internet is actually a cause of threat and react accordingly. Proper e-mail security solutions and phishing stimulation must be implemented. Changing of passwords at a regular interval is necessary to avoid hacking.

Various form of cyber–crimes are experienced by Indian women who use the internet in the contemporary context. Neither the IPC provision nor the provision of the IT Act fully reflects the ground realities that women experiences. In many situations, such as morphing E-mail, spoofing and trolling, IPC provision is applied by extrapolation and interpretation for the want of more specific provision of law. Although the IT act contains a chapter on offence, including computer-related offence, the provisions deal mainly with economic and financial issues: there is no specific provision on cyber-crimes against women even though they are rampant and are widely

reported. The leading step toward providing lawful remedies for women is to ensure that the online experience of harassment/threat/intimidation/violence caused to women is accurately translated into the written law through amendments to the two major statutes. Lastly developing confidence building mechanisms with victims and potential victims is crucial, in order to encourage crime reporting.

REFERENCES

1. P. E. Ephraim, "African youths and the dangers of social networking: A culture-centered approach to using social media," Ethics Inf. Technol., 2013, doi: 10.1007/s10676-013-9333-2.

2. R. Misra, "Cyber Crime Against Women," SSRN Electron. J., 2014, doi: 10.2139/ssrn.2486125.

3. "The criminology of cyber stalking: investigating the crime, offenders and victims of cyber stalking," Int. J. Criminol. Sociol. Theory, 2014.

4. N. Seam, "Cyber crime against Women," IMS Manthan (The J. Innov., 2015, doi: 10.18701/imsmanthan.v8i2.5130.

5. J. Lewis, "Cyber terror: Missing in action," in Technology and Terrorism, 2017.

6. M. I. Lone, "CYBERCRIME IN INDIA: A STUDY, 2007 TO 2011," Inf. Stud., 2013.

7. M. D. Cavelty Dr., "Cyber-terror-looming threat or Phantom menace? The framing of the US cyber-threat debate," J. Inf. Technol. Polit., 2008, doi: 10.1300/J516v04n01_03.

8. M. Levi, "Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change," Crime, Law Soc. Chang., 2017, doi: 10.1007/s10611-016-9645-3.

9. MarketLine, "United Arab Emirates: In-depth PESTLE insights.," MarketLine, no. October, pp. 1–84, 2018, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=133355425&amp%0Alang=es&site=ehost-live.

10. M. M. Billah, "Sufficiency of Omani Laws to Suppress Cybercrimes in Light of the un Comprehensive Study on Cybercrimes," Arab Law Q., 2018, doi: 10.1163/15730255-12321010.