Page 1877 - 1886 **DOI:** *https://doij.org/10.10000/IJLMH.112735*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 1

2022

Cyber Crimes and the Victimisation of Women

SHERIN FARHANA EV[1]

ABSTRACT

In the digital era, ICT has revolutionized each sector, and Internet usage has become an addictive act day by day. For years, there has been an increase in internet crimes against women, and the lockdown has emboldened stalkers. Technical and legal measures are being taken to protect computer systems and to prevent and deter illegal behaviour. However, due to no physical limitations, criminal activities are increasing. Even though India has enacted laws for protecting cyber offences but still crime rates are high. Cybercrime offences against women and children are at an all-time high, and they could pose a serious threat to a person's overall security. The combination of the internet and social platform are the major causes for cyber-crime against women and children. The cyber-world has united people across the world both personally and professionally, and now it has reached its highest peak, which has led to new offences, and the victims are mostly women. The internet, even though it has aided society in many positive ways, at the same time, it has paved the way for many new cyber offences. The traditional laws which regulated the society are not enough for the present scenario. According to the research conducted by the Indian computer emergency response team, one cyber-attack is reported every 10 minutes. This paper analyses the loopholes in the system with regards to handling offences related to cybercrimes on women, and it also analyses the provisions of the Indian Penal Code and Information Technology Act 2000 regarding cyber offences. Lastly, the author concludes by recommending certain necessary measures for addressing this issue.

***Keywords**: Cyber-crimes, Information technology, ICT, Cyber hacking*

I. INTRODUCTION

The Internet era has brought tremendous changes in all our lives; especially it affected the cognitive and psychological aspects of humans. The availability of every piece of information at our fingertips made people do things that were not possible a few years ago, and it has swept away the old realities and concepts. With the digital revolution era, human minds are getting captured and attracted towards various trends in technologies and social community. In India,

[1] Author is an Assistant Professor at Crescent School of Law, India.

 [ISSN 2581-5369]

all cyber-related offences are dealt with under IT Act 2000 and IPC. The crimes which are affected by women via cyberspace are cyber stalking, cyber defamation, cyber-sex, sending obscene material, trespassing in one's account without consent, privacy violation, pornography, cloning, morphing.

Cyberspace is a virtual reality I n which criminals commit crimes by impersonating others and then hiding in the same virtual area supplied by the internet. People should be aware of which aspects of their daily lives are being captured by cameras and act modestly in such situations. People's awareness of cyberculture and its downsides must also be enhanced. People must be educated about their rights. Cyber chatting among teenagers fosters close ties, friendships, and romance, all of which have a significant impact on relationships. The violence in the relationship to commit a crime eventually emerges from virtual friendship, dating, and romance. To rapidly identify the actual perpetrator, the police, judiciary, and investigative agencies must keep up with the latest innovations in web-based applications.

The legal system & regulatory bodies have a responsibility to keep up with technological advancements and guarantee that emerging technology do not become tools of exploitation and harassment. Legislation should not only protect users but also educate and inform all groups on how to use their freedom to communicate.

The women often trust the perpetrators or abusers and share their personal information. Through this, the abusers try to manipulate and misuse their greedy needs. Women and children need to be more aware of the usage of phones and the internet. Due to the pandemic stage, most schools are now functioning in an online mode. As a result, phone usage among children has increased, resulting in an increase in cyber-related offences against children too.

II. DEFINITION OF CYBERCRIME

- Cybercrime Is defined as an activity in which the computer or network is used as a tool for Criminal activity.
- Cybercrimes can be identified as illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them.
- Cybercrime, in a broader sense, are a computer-related crime, any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

 [ISSN 2581-5369]

III. TYPES OF CYBERCRIMES

(A) Cyber harassment via e-mail:

Under this kind of cybercrimes, the anonymous person sends flirty mails and harasses women. It includes blackmailing, threatening, writing love letters etc. Through fake emails, they try to torture women without revealing their identities.

(B) Cyberstalking:

This is one of the most widely discussed aspects of Internet crime in the modern era. The use of the Internet or other electronic means to stalk or harass any individual, group, or organization is known as cyberstalking. False accusations, defamation, slander, and libel are all examples. It may also include surveillance, identity theft, threats, vandalism, sex solicitation, doxing, or blackmail. Cyberstalking is defined as the cyber criminal's repeated acts of harassment or threatening behaviour toward the victim via internet services. Stalkers are motivated by one of four factors:

a) sexual harassment

b) love fixation

c) Retribution and hate.

d) Money

(C) Cyber morphing:

Morphing occurs when an unauthorized user with a false identity downloads a victim's photos and then edits them before uploading or reloading them. In this kind of cyber offence, mostly the women are victimized, as, without their consent, pictures are misused. Now, in media, we can see many cases reported on this issue, and mostly cine field actresses face this kind of issue a lot. This kind of act can be penalized under Sec. 43 and Sec. 66 of the IT Act 2000. This act also can be punishable under Sec. 509 of IPC.

(D) Cyber hacking:

When we hear the words "hacking" or "hacker," the image that comes to mind is of a clever individual that is criminal by nature, who assaults other computer systems, ruins them, breaks codes and passwords, sends viruses, and so on. Hacking is the most common type of cybercrime involving unauthorized access to a computer system or network. It's an infringement on data privacy that usually occurs in an online social community to degrade a lady by transforming her entire profile into an obscene, disparaging one. The motivations range

 [ISSN 2581-5369]

from personal animosity to a desire for vengeance to simply having fun. Even while certain social networking sites, such as Orkut and Facebook, offer features such as reporting fraudulent profiles, PhotoVideo lock, and specific reporting tools, many women are left in the dark when their email addresses or websites are hacked.

Hackers are divided into several categories. Some people use the term hacker to refer to "a skilled coder," whereas others use it to refer to "someone who tries to break into computer systems." Programmers who use their skills to cause havoc, crash machines, release computer viruses, steal credit card numbers, make free long-distance calls (the phone system is so similar to a computer system that it is a common target for computer criminals), remove copy-protection, and distribute pirated software.

(E) Cyber pornography:

Pornography is defined as the sexually explicit representation of people in words or images with the primary, immediate goal and reasonable hope of evoking significant sexual arousal in the consumer of such material. Pornography or pornographic material varies according to people's perceptions and understandings of different cultures around the world, making it difficult to define what constitutes pornographic content/material. Pornography has become a form of business in society, with people engaging in it in order to profit financially, and the victims are more of children. Another incidence occurred in Mumbai, where a Swiss couple gathered slum children and forced them to appear for obscene images, which they photographed and then uploaded to websites dedicated to paedophiles. The couple was arrested for the offence of pornography by Mumbai cops.[2]

In India, child pornography is prohibited, and it is a punishable offence under the Information Technology Act 2000 and the Indian Penal Code of 1860. The term "child" refers to anyone under the age of eighteen. Abusers use the Internet extensively to reach and sexually abuse youngsters all over the world. In India, the internet is quickly becoming a necessity. Its rapid growth has made children a viable target for cybercrime. [3]Avnish Bajaj v. State this case was decided by Justice S. Muralidhar of Delhi High Court in May 2008. It is a very well-known case of voyeurism which is also known as the Delhi Public School MMS incident of 2004. It took into account the making of a pornographic video recording of two school students engaged in sexual activity and its illegal circulation among students in the form of an MMS. Also, the

[2] G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007)
[3] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3

video was bid to auction on the website named eBay India. In the Suhas Katti v. State of Tamil Nadu case, the victim is a divorced woman who began getting texts from the accused after she rejected his marriage proposal. The accused individual utilized a fake mail id in the identity of a female to send her filthy, irritating and defamatory photographs in a yahoo chat group. People also were calling the victim by requesting sexual activities; she filed a complaint to a cyber cell on the completion of the investigation; the accused was convicted for a period of 2 years of rigorous imprisonment and a fine amounting to Rs. 500, further, one-year simple imprisonment and Rs. 500 fine, this sentence was awarded under Section 469 and Section 509 of IPC, respectively.

(F) Cyber sexual defamation:

Cyber defamation is the publication of defamatory material about another person via a computer or the Internet (social media, chat channels, or emails).To be more specific, cyber defamation occurs when someone makes a defamatory statement about another person or entity on a website, social media platform, or messaging channel or sends emails containing defamatory material to another person or entity with the intent to defame the other person or entity about whom the assertion was made. It is not a minor offence, given that it has the potential to have a significant impact on a country's economy, depending on the information and the person to whom it is disclosed. [4]SMC Pneumatics (India) Pvt. Ltd vs. Jogesh Kawatra, in this case, the company's employee sent defamatory and obscene e-mails about its Managing Director. Frequently they sent anonymous e- mails and also sent too many of their business associates to damage the image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved to the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e- mails, which are defamatory or derogatory to the plaintiffs.

(G) Cyberbullying:

Cyberbullying is described as the act of making negative comments about someone on the int ernet in order to annoy and shame them. [5]Social media sites like Facebook, Twitter, blogs, Y outube, and Instagram are examples of Internet media. The existence of social media has paved the way for a variety of criminal behaviours among humans as the reason is mainly due

[4] Misra, Rajat, Cyber Crime against Women Available at SSRN: https://ssrn.com/abstract=2486125 http://dx.doi.org/10.2139/ssrn.2486125 accessed on 15th October 2019 at 04:03pm.
[5] Fredrick, K. (2009). Mean girls (and boys): Cyberbullying and what can be done about it. *School Library Media Activities Monthly, XXV (8), 44-45.*

to lack of physical space the accused has the confidence that it's not easily traceable.

Case Law: YogeshPrabhu v. State of Maharashtra

It was the first time a conviction was handed down in any case of stalking a woman on the internet. In the beginning, in 2009, On a social media platform, a woman began speaking with the accused Yogesh Prabhu Yogesh made a proposal to her. She declined the marriage proposal. Following that, she had been receiving texts incessantly, but she had stopped. She didn't respond to them and instead ignored them, as she had suspected. His peculiar behaviour she had him blocked on the internet, so He was unable to locate her. However, he continued to follow her, and after a few months, he began sending her emails that included photos and video snippets from an unknown source. Later she filed a police report, and it was taken to a cyber cell, and IP address was tracked, and it was found he was sending a message from his office, and the accused was arrested under Section 509 of IPC and Section 66E of the IT Act.

IV. CYBERCRIMES PROVISIONS UNDER IT ACT & IPC

[6]Cybercrimes which is addressed by the IT ACT of 2000 are:

- Sec 65. Tampering with computer source documents.
- Sec 66. Computer-related offences.
- Sec 66A. Punishment for sending offensive messages through communication service, etc.
- Sec 66B. Punishment for dishonestly receiving stolen computer resources or communication devices.
- Sec 66C. Punishment for identity theft.
- Sec 66D. Punishment for cheating by personation by using computer resource.
- Sec 66E. Punishment for violation of privacy.
- Sec 66F. Punishment for cyber terrorism.
- Sec 67. Punishment for publishing or transmitting obscene material in electronic form.
- Sec 67A. Punishment for publishing or transmitting of material containing the sexually explicit act, etc., in electronic form.
- Sec 67B. Punishment for publishing or transmitting of material depicting children in

[6] Information technology Act 2000

 [ISSN 2581-5369]

the sexually explicit act, etc., in electronic form.

Under [7]the Indian Penal code, the offence of cybercrimes can be charged under:

- Sending Threating Messages by Email, Indian Penal Code (IPC) Sec.503.
- Sending Defamatory Messages by Email, Indian Penal Code (IPC) Sec.499
- Forgery of Electronic Records, Indian Penal Code (IPC) Sec.463
- Bogus Websites & Cyber Fraud, Indian Penal Code (IPC) Sec.420
- Email Spoofing, Indian Penal Code (IPC) Sec.463
- Email Abuse, Indian Penal Code (IPC) Sec.500
- Stalking (IPC) Sec.354D
- Printing, etc. of grossly indecent or scurrilous matter (IPC) Sec.292A

V. SOCIAL MEDIA AND CYBER CRIMES

Women all across the world have been subject to technology crimes like morphing, bogus pr ofiling, and cyberbullying as a result of the rise of social media platforms. Social media can be used and accessed by anyone regardless of their economic, social or political background. With more technological advancements, all types of Social media are in one click.

Though the regulations of the IPC and the Information Technologies Act attempts to prevent t hese crimes to some extent, their effectiveness still remains in question. Social media like Instagram is a major social media platform today. Instagrams advantage is the multimedia content of images and videos as well as the features which allow the users to express comments to one another. Users can rapidly share photographs and videos, which can be accessed by users. Due to the updated information on Instagram and Facebook, information's like personal details are easily available to the perpetrators. [8]The experience of cyber offences is possibly intensified from the experience of the playground bully for several reasons: the target's experience appears to be intensified because the perpetrator can hide behind a screen name and can act without fear of punishment. [9]Globally, attacks are most common on Facebook, where 39% have suffered harassment, followed by Facebook (30%), Instagram (23%), WhatsApp (14%), Snapchat (10%), Twitter (9%) and TikTok (6%).

[7] Indian Penal code 1860

[8] Lori O. Favela, *Female Cyberbullying: Causes and Prevention Strategies*, available at: http://www.inquiriesjournal.com/articles/322/female-cyberbullying-causes-and-prevention-strategies

[9] https://www.theguardian.com/society/2020/oct/05/online-violence-against-women-flourishing-and-most-common-on-facebook-survey-finds.

 [ISSN 2581-5369]

VI. REASONS FOR THE GROWTH OF CYBERCRIMES ON WOMEN

The steep increase of cyber-crimes on women and children are due to following

- Availability of personal information
- Chatting/Dating via social platforms
- Lack of privacy
- Lack of knowledge on technological advancement
- Negligence on safety measures
- Lack of strict laws on Internet service providers
- Strict rules have to be brought upon cyber café running
- Lack of awareness over cyberculture
- Virtual friendships & Depression
- Addiction towards games
- Hiding identity under fake profiles
- Lack of uniform laws, conventions

Most of the cyber-crimes on women and children are unreported due to the social stigma and fear of defamation.[10]Every human being has the urge for knowledge, and this urge has made man discover the path of technological advancement.

In India, cyber-crimes against women and children includes both sexually and mentally. The police and the system should be availed information with the latest development in web-based applications so that they can quickly trace the accused.[11] The legal system should be on par with technological growth. Otherwise, it gives the freedom and platform for the accused. The level of the problem originated from the information and communication technology remains more or less similar across the world. A recent study shows that the number of internet users has been increased to 75 million. Even though the preamble of the IT Act 2000 has dealt with commercial and financial crimes, it lacked the safety of Internet users.

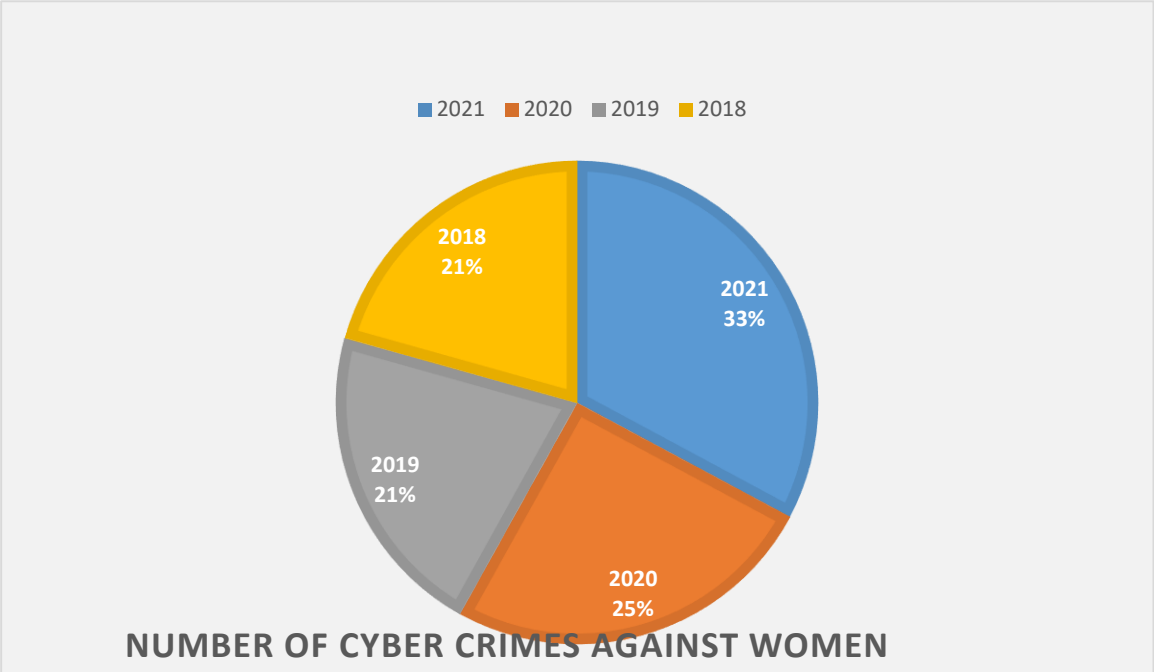
[12]When India started the journey of protecting electronic transactions, priority was given for

[10] Misra, Rajat, Cyber Crime against Women,Available at SSRN: https://ssrn.com/abstract=2486125 or http://dx.doi.org/10.2139/ssrn.2486125

[11] C.J. Magnin, An Efficient Tool to Fight Crime in Cyber-space? The Council of Europe Convention on Cyber Crime, (2001).

[12] Danielle Keats Citron, Law's Expressive Value in Combating Cyber Gender Harassment, 108(3) Michigan Law

protecting e-commerce, and no safety measures were recommended for socialized cyber communication.



VII. SUGGESTION

- A proper legal system should be brought when it comes to cross border issues, and the law enforcement agencies and police forces must be made aware of the difficult aspects of cybercrime against women and children, as well as their dimensions, in order to better record and respond to such crimes.
- Women should be given a platform to report their complaints online using a Digital Police Portal or E-Portal. This could minimize the number of cases that go unreported due to the stigma attached to them and the tendency of parents and guardians to avoid involving the authorities in such circumstances.
- The portal also keeps a criminal database, which might be extremely useful to law enforcement, and a system of awareness programmes should be brought in schools regarding cyber offences for awareness for children.

Other than the above suggestions, every woman should be cautious with the below following points:

- Password management should be securely handled
- Avoid revealing personal information to strangers

Review, 373-415 (Dec., 2009).

 [ISSN 2581-5369]

- Be alert and Cautious in online chats
- Understand privacy settings
- Antivirus update
- Keep firewall turned on
- Being aware of new security threats
- Avoid using the same password for multiple accounts
- Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.

VIII. CONCLUSION

Cyber-crimes faced by women is a major issue, and it's found that due to technological development and exposure, combating cybercrime against women, in general, is difficult. To overcome all of these obstacles, the government must strengthen the legal system by enforcing current laws in accordance with societal needs, thereby creating awareness and also by enforcing a strict punishment policy, a strong law and legislatures.

*****

 [ISSN 2581-5369]