LawPublicus

The Legal Portal

Volume 1 : Issue 2

2021

January 2021

Email ID: Lawpublicusportal@gmail.com

Website: www.Lawpublicus.com

Address: A18 Dayanand Colony Lajpat Nagar - 4

New Delhi

Disclaimer

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of ***LawPublicus*** The Legal Portal. The Editorial Team of ***LawPublicus*** holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of ***LawPublicus***. Though all efforts are made to ensure the accuracy and correctness of the information published, ***LawPublicus*** shall not be responsible for any errors caused due to oversight or otherwise.

FOR *LawPublicus* The Legal Portal

Editorial Team

About Us

LawPublicus The Legal Portal is a leading journal of multidisciplinary research. It is a free, peer-reviewed, open-access journal that provides insight into diverse and dynamic legal matters.

LawPublicus is a novel initiative by legal minds. As the its name suggests, it is platform for young minds to ignite their willingness and inventiveness in order to contribute to the field of law through new ideas, opinions and thereby contributing to an informed citizenry.

We hope to provide a forum for young and enthusiastic writers to voice their feelings and research on interdisciplinary approaches. We also have in view to evaluate, explore and deliberate, under the tutelage of seasoned editors and academic experts, on current trends and projections based thereon in legal studies. LawPublicus focuses not only on the scholarly writings but also on numerous other approaches such as discussions, interviews, and debates with experts and qualified & industrial professionals.

We are determined and excited to bring authentic, creative and individual ideas and socially-related problems into attention.

LawPublicus calls for research papers, articles, short notes, book reviews & case commentaries, that are distinctive and unpublished.

With this thought, we hereby present to you

LawPublicus The Legal Portal

The Need of Cyber-Security for Women and Girls

Authored By:
Mili Kanoujiya
Designation: Student B.A. LL.B. (Hons.), Vth Year
Law College Dehradun, Uttaranchal University, Dehradun
E-mail ID: Milikanoujiya@gmail.com
Contact: +91-84499952**

THE NEED OF CYBER-SECURITY FOR WOMEN AND GIRLS

Mili Kanoujiya

ABSTRACT

The expeditious progress in mobile apps and web innovation has given rise to severe risk to the privacy and security of individuals. No one is safe in the cyber-world but most often the females become the victim of the viciousness of the cyber world. The development in the internet facilities has extended the scope of interference with the privacy of women and girls at online platforms. Consequent to which the rates of cyber-crimes against women are up surging. This article aims to understand different kinds of cyber-crimes against women and girls, the reasons and impacts of it. It also focuses on the laws available that punishes cyber-crime and throws light on some of the recent instances of cyber-harassment of women and girls. The author has tried to suggest some of the ways in which the females can stay safe in cyberspace.

INTRODUCTION

In simple words, cybercrime is an illicit activity which is done with the aid of computer and internet. It is not expressly elucidated in any legislation. In India, there are no particular laws for the protection of women from the invasion of their privacy in cyberspace. Cyberspace has gained extreme significance during the past few months. A considerable number of people have switched to online mode for socializing, working etc. Life has become simple but several threats for the netizens have arisen. There has been a hike in cybercrimes against women in India. At the present times, women and girls are not at all safe either offline or online. Cybersavary has grown a lot that abuse has become a day-to-day reality for girls.[1] There have been different social media sites inclusive of Facebook, Instagram, YouTube, TikTok etc, used by people for the purpose of leisure. These sites contain a large number of user generated contents which are tremendously absorbed by others. Several contents are created at the social media platform clearly for the purpose of harassing women and girls.[2]

Cybercrime has been rising at an alarming rate in recent times and possibly it is the most complicated issue in the world that needs prompt consideration and reassuring methodologies from the society, government, families and individuals.[3] 71 Crore Indian population depends on the web services, among which, 25 crore are females. 80% of the population is becoming victims of cyber offences and 63% of them don't have any idea where to register complaints on cyber-crimes.[4] A total of 412 bonafide complaints of cyber abuse within the lockdown period from March 25 till April 25 were received. Amongst these, around 396 complaints were real from female victims, ranging from "abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands,

[1] Melissa Davey, "Online violence against women 'flourishing', and most common on Facebook, survey finds" available at https://www.theguardian.com/society/2020/oct/05/online-violence-against-women-flourishing-and-most-common-on-facebook-survey-finds accessed on 10/12/2020.

[2] Dr. Debarati Halder, "Covid-19 lockdown and cyber victimization of women" available at https://debaraticyberspace.blogspot.com/ accessed on 15/12/2020.

[3] S. Poulpunitha, K.Manimekalai, P.Veeramani, "Strategies to prevent and Control of Cyber Crime against Women and Girls", available at http://www.ijitee.org/wp-content/uploads/papers/v9i3/K24080981119.pdf accessed on 27/11/2020.

[4] Cyber-crimes against women on the rise, available at https://www.thehindu.com/news/national/andhra-pradesh/cyber-crimes-against-women-on-the-rise/article32399536.ece accessed on 01/12/2020.

blackmail and more".[5] As told by the Ministry of Electronics and Information Technology (MeitY) to the Parliament that "till August 2020, Indian citizens, government and business entities faced around seven lakh cyber-attacks. As per their estimates, Rs 1.24 lakh crore was lost due to cybercrimes in India amid the last year."[6] There is a need to spread enormous awareness with respect to how to remain secured in the cyber world.

TYPES OF CYBERCRIMES

Cyber Crimes against women are of different types. The major types are discussed as follows:

Cyber Stalking: This crime is reported most often by women. In this type of crime the wrongdoer tracks the movement and activity of a woman. Most of the time it is done by men by means of the internet via emails or other medium of messaging. It also includes posting offensive comments[7] on the internet about an individual. Such sort of action is done repeatedly to the victim. It is not a difficult task for a cyber-stalker to pick up private data of any individual within minutes. There are four reasons behind cyber stalking particularly: "sexual harassment", "revenge and hate", "obsession love", and "ego and power trips".[8]

Cyber Defamation: Defamation is already a civil and criminal wrong. When it is committed by utilizing computer and web resources by publishing such statements or materials that have the capacity to defame the other individual, it is called cyber defamation. The reason being, the large number of internet users due to which any defamatory statement or material go viral within very less time. Thereby, affecting the dignity of the victim. Consequently the victims have to suffer humiliation in the actual world.

Non-Consensual Pornography: This is one of the foremost serious crime on the internet against women and girls. The pictures or video clips of a victim are used without their assent

[5] Significant Increase in Cyber Crimes against women during lockdown: Experts, available on https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352 accessed on 20/11/2020.

[6] Aarti Tikoo Singh, "India approves game-changing framework against cyber threats" available at https://www.expresscomputer.in/egov-watch/india-approves-game-changing-framework-against-cyber-threats/70412/ accessed on 18/12/2020.

[7] Available at https://eige.europa.eu/documents/cyber_violence_against_women_and_girls accessed on 25/11/2020.

[8] Jaspreet Singh, "Violence against Women in Cyber World: A special reference to India", available at https://garph.co.uk/IJARMSS/Jan2015/8.pdf accessed on 27/11/2020.

and duplicated in an obscene material. This can be very traumatic for any woman. Most of the time it is the result of revenge porn, where the perpetrator is the known person of the victim. There are various examples of this type of crime, one of which is DPS MMS Scandal, where an MMS was made of a school girl and it was circulated on the internet.

Cyber Harassment: This incorporates persistently sending love letters or vulgar messages by hiding real identity via fake ids over the internet, blackmailing and threatening to leak intimate content of women. The motive behind such acts is to force the women in undesirable sexual activities. This also includes harassment by cyber bullying.

Morphing: In this category of cyber-crime an unauthorized user edits the original picture of the victim. It is done mostly by using a fake identity to download the victim's picture and then uploading them again on the internet after editing.[9] Most often the offender creates explicit content by editing the face of the victim woman on a bare body of another. This sort of activity outrages the modesty of the women and girls.

REASONS FOR RISE IN CYBER CRIMES AGAINST WOMEN

In India, the privacy and security of women is at high risk. Personal information of individuals can be easily availed through social networking sites. Such information can be abused by any individual. Not all the women using social networking sites are well-informed with respect to how they can keep up their protection on social media. Most females overlook to go through the rules and regulation to protect privacy on social media. The offenders hide their genuine identity and use fake identity on social media. Most of the time the victims are not aware about where and how to report these crimes. It can be said that the rise in such crimes is due to the need of proper knowledge about how to use social media in a secure manner and the need of effective laws for the protection of women. It is hard to know the jurisdiction in which the crime is committed. Lack of awareness about how and where to report cybercrime additionally lack confidence in the police department. Even the police officials do not pay much attention to such complaints by female victims.

[9] Available at https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf accessed on 12/11/2020.

IMPACT OF CYBERCRIMES

Cybercrimes like several other forms of crime have a huge impact on the victim as well as on society. Primarily, the victim ought to suffer the impact of cybercrimes which may vary from stress, depression or mental shock. Most of the time it can compel women to commit self-harming action. Also, the discrimination from the society if the woman falls a victim for cyber pornography or cyber defamation.

LAWS DEALING WITH CYBERCRIMES

The Constitution of India under the purview of Article 21 provides for Right to Privacy which is available to every individual. The cyber-crimes occurring with women is a gross violation of their right to privacy and disrespectful to the dignity of women. There is no specific law that aims to curb cyber-crime against women. However, certain provisions are available in different legislation to protect individuals from cybercrimes. There is no law to protect women against verbal abuse and harassment that do not involve sexually explicit content. There is again no law to protect women from psychological violence.

Section 354A- This section deals with Sexual harassment and prescribes punishment for it. "A man committing any of the following acts such as physical contact and advances involving unwelcome and unexplicit sexual overtures; or a demand or request for sexual favors; or showing pornography against the will of a woman; or making sexually coloured remarks, shall be guilty of the offence of sexual harassment." The person shall be punished with imprisonment or with fine or both.

Section 354C- This Section deal with punishment for 'Voyeurism' as "Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed by either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image 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, and shall also be liable to fine, and 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 which may extend to seven years, and shall also be liable to fine".

Section 354D- Defines 'Stalking' as any person who "follows a woman and contact or attempt to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking. On first conviction the punishment is imprisonment of either description for a term which may extend to three years, and shall also be liable to fine. On second or subsequent conviction the punishment shall be imprisonment of either description for a term which may extend to five years, and shall also be liable to fine."

Section 499- This Section deals with Defamation. It lays down, "whoever, by words either spoken or intended to be read, or by signs or by visible representation, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person".

Section 500- This section prescribes a simple imprisonment upto 2 years with or without fine.

Section 503- This section deals with Criminal Intimidation, which is defined as "Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threats, commits criminal intimidation".

The Information Technology Act, 2000 prescribes the punitive measures for cybercrimes. Both imprisonment and fine are incorporated in it as punishment. Punishment for identity theft is provided under Section 66C for the dishonest and fraudulent use of "electronic signature, password or any other unique identification feature of any other person". Section 66E makes punishable the capturing, publishing or transmission of images of private parts of any individual, without their assent. The "publishing or transmitting of obscene material in electronic form" is made punishable under Section 67. The "publishing or transmitting of material containing sexually explicit acts, etc., in electronic form" is punishable under Section 67A. The "publishing or transmitting of material depicting children in sexually explicit acts, etc,. in electronic form" is punishable under Section 67B.

Indecent Representation of Women (Prohibition) Bill, 2012- controls and banned the representation of women in an indecent manner through the media of advertisements[10], publications etc. The purpose is to bring under the umbrella of law, the audio-visual media and content in electronic form, and dissemination of material including dissemination and the portrayal of women on the internet.

Even after there are ample laws that can control cybercrime to certain extent but they are ineffective. The conviction rate for crime against women on cyberspace is extremely low. The laws are not effective enough to cause any deterrence in the minds of the offenders. There is a need for a separate legislation to deal with new emerging cyber-crimes against women and strict implementation is to be ensured in order to create a safe space for women online.

CERTAIN INSTANCES OF CYBERCRIMES AGAINST WOMEN

In Suhaskutti v. State of Tamil Nadu[11], defamatory messages were posted regarding a divorcee lady in the yahoo message group which gave people a belief that she is soliciting. That resulted in multiple annoying phone calls to the lady. Conviction was done under Section 67 of the Information Technology Act, 2000.

The Air force Bal Bharti School Case[12], was the first case of Cyber pornography in India which was registered in Delhi juvenile court. The accused who was a student in Class 12th created a website for the sake of revenge that contained explicit content relating to his girls schoolmates and teachers. For this act he got suspended by the school authority and charged under Sections 292, 293, 294 of IPC, Section 67 of the IT Act, 2000 and Indecent Representation of Women Act.

In Dr. L. Prakash v. Superintendent[13], women were forcefully demanded to perform sexual acts by an orthopedic surgeon (accused), which he used to record and circulate as entertainment materials for adults on the internet. He was arrested under Section 506, 367 and 120-B of Indian

[10] Section 3, The Indecent Representation of Women (Prohibition) Act, 1986.
[11] Suhaskutti v. State of Tamil Nadu, 4680 of 2004 Criminal Complaint.
[12] The Air Force Bal Bharti, Delhi Cyber Pornography Case 2001.
[13] Dr. L Prakash v. Superintendent (Madras High Court, W.P. 7313, 2002).

Penal Code and Section 67 of IT Act, 2000. He got punishment of life imprisonment along with a fine of Rs 1,25,000 under the Immoral Trafficking (Prevention) Act, 1956.

In the case of Saddam Hussain v. State of Madhya Pradesh[14]The accused offended the modesty of a female, video recorded the incident in his phone and used it to blackmail the victim. A criminal complaint was registered under Section 354D and Section 507 under IPC for Stalking and Criminal Intimidation by anonymous communication respectively and also under Section 66A of the IT Act. Later, a petition was presented before the Madhya Pradesh High Court for suppressing the case on the basis of a compromise arrived at between the victim and the accused. The High Court treated the act committed as a serious offence and refused to quash the proceedings.[15]

Bois Locker Room incident: A group on Instagram named Bois Locker Room was created by 10-15 boys using fake ids. Offensive and obscene photographs of underaged girls were circulated in the group and the boys used to make vulgar and fake remarks on their bodies. The boys involved were school going children from very financially powerful families. The boys made rape threats to those girls who approached them regarding those photographs. The screenshots of the chat including rape threats went viral on the web and it then became a serious matter. The Delhi Police Cyber Crime took cognizance of the matter. The admin of the group was arrested who was found to be a student of 12th Class.[16] The Delhi High Court, issues notice to Central Government, Facebook, google and Twitter on a plea which laid forward directions to social media companies to eliminate any illegal groups available at their platforms so as to ensure 'safety and security of children' in cyberspace, further the plea stated that these social media platforms would be held liable under the IT Act, 2000 along with POCSO Act, 2012.[17]

[14] Saddam Hussain v. State of Madhya Pradesh 2016 SCC Online MP 1471 (India).

[15] Ms. Saumya Uma, "Outlawing Cyber Crimes against Women in India", available at https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf accessed on 25/11/2020.

[16] Bois Locker Room probe: Minor girl created fake character, say Delhi Police available at https://www.timesnownews.com/mirror-now/crime/article/new-twist-in-bois-locker-room-case-juvenile-girl-created-fake-profile-to-test-boys-say-delhi-police/589894 accessed on 28/11/2020.

[17] Aditi Singh, "Delhi HC issues notice in plea seeking removal of illegal groups from social media platforms for safety and security of children" available at https://www.barandbench.com/news/litigation/delhi-hc-issues-notice-in-plea-seeking-removal-of-illegal-groups-from-social-media-platforms-for-safety-and-security-of-children accessed on 27/11/2020.

Promotion of acid attack by an influencer on TikTok- Tiktok being a popular app is used by a lot of students including students, amid this lockdown phase. Faizal Siddiqui with around 13.4 million followers on that app made a video that encouraged acid attacks. The complaint was registered immediately by NCW and TikTok India was asked to take down the video as it was "promoting the grievous crime of acid attack on social media".[18] TikTok has most often been a stage for the commission of cyber-crimes against women. Madras High Court about a year ago prohibited TikTok expressing that it can be utilized to circulate explicit contents widely, exposure for children to disturbing content etc. This boycott was however lifted, yet there are still various videos being circulated which glorify rape culture and different other crimes against woman.

HOW TO OBTAIN REMEDY?

The victim of cyber-crime at first should contact the nearest police station or cyber cell, if any. The victim may also register an anonymous complaint on cybercrime.gov.in (National Cyber Crime Reporting Portal). The victim has to provide a certain document while registering the complaint of alleged cyber-crime. In case of Harassment through emails the victim has to provide the soft copy and hard copy of that particular offending mail. The victim must not delete that email so as to keep that as a proof for obtaining remedy. The victim may also give the list of suspects, if any.[19] Toll free number 112 can also be utilized for reporting cybercrime.

SUGGESTIONS TO TACKLE

It is suggested to not disclose any personal information on the internet. Passwords must be changed on a regular basis and must not be shared with anyone. Before using any of the social media apps, it is advised to go through its terms and conditions. It is better to refrain from sending personal photographs to friends or strangers on the internet as it can be misused very easily.

[18] Medha Chawla, "TikTok removes Faizal Siddiqui's video promoting acid attack after NCW complaint", available at https://www.indiatoday.in/trending-news/story/tiktok-removes-faizal-siddiqui-s-video-promoting-acid-attack-after-ncw-complaint-1679233-2020-05-18 accessed on 25/11/2020.

[19] Cyber Crimes against Women, available at https://vikaspedia.in/social-welfare/women-and-child-development/women-development-1/legal-awareness-for-women/cyber-crimes-against-women accessed on 28/11/2020.

Women empowerment is very necessary to protect them from any type of crimes including cybercrimes. Women must keep themselves well aware of how to be technologically secure and also the legal process and framework, if they fall prey to such crimes. Females have to understand the difference between distrust and mistrust. Capacity building, preparedness and taking all necessary precautions can help females to tackle cyber-crimes.

The law enforcement agencies must remain updated with the most recent development within cyberspace so that real perpetrators can be recognized quickly. The law formulating agencies must keep pace with the advancement in technology so as to ensure that such technology should not be used as a tool to exploit or harass people. It must be taught to every individual to respect the rights and privacy of other individuals.

CONCLUSION

It's a mere illusion for a woman to think of a secure space for herself as the rates of cyber-crimes against women are increasing rapidly. The plight of women ought to be improved and it requires crime against women to be taken seriously especially the widely expanding cybercrimes. Stricter punitive measures are required to be introduced for the cyber offenders. Education regarding the healthy practices in cyberspace is required to be introduced in schools. It is the responsibility of every individual to respect the privacy of other individuals and not to breach it.

Recently on 16 December 2020, the first and biggest framework was presented in India for the purpose of securing itself from the varying ranges of cyber threats. The Union cabinet has validated the 'National Security Directive on Telecom Sector' taking into account the daunting magnitude of cyber threats to India.[20] It can be expected that this framework will help in controlling cyber-crimes.

---

[20] Aarti Tikoo Singh, "India approves game-changing framework against cyber threats" available at https://www.expresscomputer.in/egov-watch/india-approves-game-changing-framework-against-cyber-threats/70412/ accessed on 18/12/2020.