ISSN: 2582-2942

LEXFORTI

Legal Journal

Vol-II Issue- I

October, 2020

I S S N : 2 5 8 2 - 2 942

DISCLAIMER

ISSN: 2582-2942

EDITORIAL BOARD

ISSN 2582 2942

ISSN: 2582-2942

EDITORIAL BOARD

ISSN: 2582-2942

ABOUT US

LexForti Legal News and Journal offer access to a wide array of legal knowledge through the Daily Legal News segment of our Website. It provides the readers with latest case laws in layman terms. Our Legal Journal contains a vast assortment of resources that helps in understanding contemporary legal issues. LexForti Legal News and Journal also offers Certificate courses. Whoever register for the course is provided the access to the state of the art E-portal. On completion of all the module and Test, candidate will be given Certificate of Accomplishment of Course. Be sure to make the most of it. LexForti Legal News and Journal is also proud to announce that we have made India's first Legal News android application which contains Daily Legal News, Legal Journal and Certificate Courses, everything in 4 MB.

Cyber Crime Against Women: A Cyber Exploitation

Vartika Vasu, Krishnapriya.G

ABSTRACT

Cyberspace has become a boon for human society. Internet has linked people around the world. The social networking sites have developed new sphere for socializing. Women in the society are enjoying liberation irrespective of any discrimination. Women are using these sites as a stress reliever for their emotional needs and personal problems. But are they enjoying these liberation in true sense? On one side internet is serving as boon whereas on the other side it has created insecurity for the women due to rising cyber crimes. India is a patriarchical society where women are victimised as well as blamed and online victims are no exception. There are many instances where women face social stigma due to online victimization.

This research paper throws light and discusses various kinds of cyber crimes committed on women and how it affects them negatively. This paper shall discuss about the various cyber crimes against women such as ***online grooming, trolling, privacy infringement, pornography, sexual defamation, morphing, online stalking*** *and so on. This paper shall also examine the various case laws which exist to protect women's right such as the* ***Information Technology Act (2000) and*** *several sections which have been amended under the* ***Criminal Amendment Bill (2013).*** *This paper shall also include the infamous* ***Ritu Kohli Case*** *and various other cases like* ***Karan Girotra v. State & Anr, Puri Cyber Pornography Case*** *and other such cases.*

Through this paper, the authors intend to suggest remedies for the cyber crimes being comitted against women in India. In the conclusion it will focus upon various measures which can be taken and the reforms needed in the legal system to curb the escalation of cyber criminals.

INTRODUCTION

"*Time is now here to exculpate that our women are safe in cyber world, the memento alarms to stop tomfoolery activities on internet access as it is an offence and women take umbrage from it.*"[1]

The online surface has now become a path where a woman's status, privacy and safety is being questioned every moment. According to the data, every second a woman in India is being targeted to be victimized of cybercrimes. The patriarchy present in the roots of the Indian society has victimized a woman as well as blamed them.There are so many instances where women face social stigma due to online victimization. The effect of these cybercrimes against women is more mental than physical harm. Somehow, it is valid to say that the National Crime Records Bureau [NCRB] of India does not keep any separate records of cybercrimes registered against women. As the focus of the laws that secures the safety of the woman is more on physical than mental harm. Most of the cybercrimes remain unreported due to the hesitation as well as the unawareness of the women as to where to report such crimes.Some of them are not quite serious about reporting such crimes due to the risk of social embarrassment. Some of the large cybercrimes have put a huge number of women into different kind of serious health issues such as depression, anxiety, hypertension, other heart diseases etc. These cybercrimes are mainly perpetrated by the male section of the society with malafide intention such as to insult, taking revenge, blackmailing, sexual harassment, statisfaction of gaining control by using online platforms. The mindset of the women requires to be widen up to curb these crimes. Most of the problems can only be solved when women lodge complaints immediately and take strong legal actions against the culprit.

[1] Dhruti M Kapadia, Cyber Crimes Against Women And Laws In India,(Nov 21, 2018, 06:06 GMT), https://www.livelaw.in.

DEFINITION OF CYBERCRIME

The term cybercrime is not new as it came to existence with the expansion of technology all over the world. Even the Indian legislature and the Information Technology Act, 2000 that deals with cybercrimes does not keep an accurate definition of the term cybercrime. The rapid increase of technology in daily life brought convenience for the users. But everything has its darker side too.

Although there is no precise definition of cybercrime, it can generally be defined as an illegal activity committed with the help of computer or other sources such as mobile or internet. There are no such definite definitions of cybercrimes, even though different institutions and personalities have given numerous definitions.

Professor S.T Viswanathan has given three definitions in his book **The Indian Cyber Laws with Cyber Glossary** is as follows –

1. Any illegal action in which a computer is the tool or object of the crime that is any crime, the means or purpose of which is to influence the function of a computer.

2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain.

3. Computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data.[2]

Later, the cybercrimes increased and expanded on the basis of gender bias victimising the women. This free flow of internet over long distances started giving rise to abundance of irresponsible behaviour towards women. But till that time there is no such recognised laws or meaning of cybercrime against women had defined.

Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "crimes targeted against women with a motive to intentionally harm the victim pshychologically and

[2] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81.*

physically, using modern telecommunication networks such as internet and mobile phones.[3]

[3] Vishi Aggarwal & Ms. Shruti , CYBERCRIME VICTIMS: A COMPREHENSIVE STUDY , 6 IJCRT,640,2018.

TYPES OF CYBER CRIMES AGAINST WOMEN

With the advancement of technology the crimes in cyber space is also increasing day by day and the cybercrimes against women are at alarming rate. Amongst various cybercrimes committed against an individual, the cybercrimes mainly targeting the women of the society at large are as follows:-

CYBER STALKING:- Cyber stalking is the most common internet crime presently. Cyber stalking generally means following a person's movements online using internet which involves sending messages or sometimes threatening constantly. Cyber stalking are usually done by the men whose targets used to be women who are emotionally weak or unstable. Over 75% of the cyber stalking victims are females. The stalker tries to approach the victim's personal information like name, family, address to harass and blackmail them. There are four major motives behind cyber stalking, for sexual harassement, for revenge in love failure, for ego and power and due to development of hatred towards someone.

CYBER DEFAMATION:- Cybercrime that includes defamation is another common internet crime against women. Even though it can happen to both genders but females are more attacked. Cyber defamation generally takes place when someone publishes defamatory information or sends defamatory messages or emails about someone with the help of computer or the internet publicly.

CYBER PORNOGRAPHY:- Cyber pornography is another threat to the female netizens. This includes pornographic websites containing porn photos and porn videos and their transmission.Internet has provided a platform for the facilitation of crimes like pornography. About 50% of the websites shows pornographic and obscene materials today. Females of the society are being threatened on the name of pornographic sites to get sexual favours or to take revenge from them.These offences mainly includes morphing of photos with nude photographs and uploading them to pornographic sites. The easy availability and access to these sites has led to more serious offences in the cyber world. Various cases related to these offences have also been reported.

MORPHING:- Morphing commonly means editing of the original picture by an

unauthorized user. It is generally done by an unauthorized user or a person with fake identity who downloads the original picture of the victim's and uploads it after editing. It was observed that the female's pictures are more downloaded by the fake users and reposted after editing. This crime is done for the purpose of blackmailing or cheating the victim's online intended to take revenge or defame them.

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.

ONLINE TROLLING:- Trolling means posting provocative or off-topic messages in online community such as newsgroup, blogs, social media (twitter or facebook) which mainly targets the females intending to emotionally upset them. It is done by the trolls who are professional abusers who create a scene of cold war by creating fake ids and using them for this purpose.

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.

CASE STUDY

Cybercrimes came into existence with the evolution of technology. These cybercrimes were not only limited to the common crimes known to everyone like hacking, frauding, or cheating but was committed against women also. But most of the cybercrimes remain unreported till that time because of the unawareness as well as the hesitation of the women as to where to report such crimes. The first ever cybercrime against women was reported in the year of **2000** that was the infamous ritu kohli case.

1. **RITU KOHLI CASE:-** It was the first reported cyber sex crime in India. It was reported on **Sunday, June 18, 2000** in Delhi. In this case a 30-year-old software engineer, Manish Kathuria, was arrested by officials of the Crime Branch of the Delhi police for harassing a woman by chatting on the internet. Manish reportedly used to chat on website www.micr.com under the name of Mrs. Ritu Kohli. He used obscene languages while chatting and also gave her residential telephone number for further chatting. As a result, Mrs. Kohli started getting obscene calls at her residence. Due to the disturbances, Mrs. Kohli lodged a complaint and after the enquiries the Delhi police traced the culprit and started criminal proceedings against him under section 67 of IT Act with section 509 of IPC for outraging Ritu Kohli's modesty.[4]

2. **STATE OF TAMIL NADU V. SUHAS KATTI:-** This is the case related to posting of obscene, defamatory and annoying message about the divorcee woman in the yahoo message group. E-mail's were forwarded to the victim by the accused through a false email account opened by him in her name. The posting of the messages resulted in online harassement to the victim as annoying phone calls started coming to her in the belief that she was soliciting. Therefore she, lodged a complaint in the Egmore Court in Feb 2004. Based on the complaint, the Chennai police cyber cell traced and arrested the accused. Further the accused found guilty of offences under section 469/509 0f IPC and section 67 of IT Act,

[4] Vishi Aggarwal & Ms. Shruti , CYBERCRIME VICTIMS: A COMPREHENSIVE STUDY , 6 , IJCRT, 646, 2018.

2000 and convicted.[5]

3. **KARAN GIROTRA V. STATE & ANR:-** This case was reported on 8th May 2012 on cyber stalking when the petitioner filed an appilication to grant anticipatory bail. This case dealed with a woman, Shivani Saxena, whose marriage couldnot be consummated and she filed a divorce with mutual consent. In between, she came across Karan Girotra while chatting on the internet, who told her that he loved her and wanted to marry her. Girotra invited Saxena over to his house to introduce her to his family where he intoxicated her and sexually assaulted her. He started assuring her that he would marry her and began sending her obscene pictures of her assaultation. He also threatened her to circulate the pictures if she would not marry him. As a result, an engagement ceremony was performed after which he continued to assault her and called off his engagement to her. Frustrated out of this, Saxena filed a complaint under section 66-A of the IT Act. Although the court rejected the plea of anticipatory bail but did not give serious custodial interrogation[6]

4. **PURI CYBER PORNOGRAPHY CASE:-** This was the first cyber pornography conviction case in the state of Odisha. The accused Jayant Kumar Das, RTI activist created a fake E-mail account and fake profile of the wife of the complainant Biswajit Patnaik, a journalist to take revenge on him. He linked the fake profile to an America based porn website and posted vulgar remarks. He also posted the victim's phone number on the porn portal. Later, the journalist lodged an FIR against Das at Baselisahi police station in Puri in July 2012 after getting obscene messages and phone calls. The Cyber Cell of the Crime Branch took over the investigation in August 2012 and arrested Das 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 the section 292 (obscenity), 465 (forgery), 469 (forgery for the purpose of harming reputation) and 500 (punishment for defamation) of the IPC and 66C/67/67A of the Information Technology Act.[7]

5. **DR. PRAKASH V. STATE OF TAMIL NADU; AIR 2002 SC 3533:-** It is the first case to

[5] State of Tamil Nadu v Suhas Katti – Cyber law case in India, indiankanoon.org.
[6] Aravinth balakrishnan: Challenges In Regulating Cyberstalking At The Cyber Space, www.legalserviceindia.com
[7] First cyber pornography case conviction in State, the pioneer (Aug 05, 2017), www.dailypioneer.com.

be prosecuted under IT Act in the State of Tamil Nadu. The case is a big scandal, involving sex, pornography, the internet and a mastermind, allegedly a medical doctor. Doctor was involved in the offences of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to 23 countries, spoiling life of many young girls, who was then kept to detention.[8] The story revealed when the city police received a complaint from Ganesh who claimed to be a victim of the doctor. Two cases got lodged against the doctor; one under Information Technology Act and the other under Arms Act. As per section 67 of the IT Act, that 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 upto 10 years imprisonment with a fine of Rs. 2 lakhs on the second conviction. Presently, six teams of police are working day and night to gather more information related to it.[8]

LAW ENFORCEMENTS

Various laws have been made for women's protection from cybercrimes under IT Act, 2000 and laws are amended under Criminal Amendment Bill, 2013. Some of the laws are as follows:

- **SECTION 66A** - Any person who sends offensive messages through communication service that causes annoyance, inconvenience, danger etc through an electronic device to mislead or deceive the recipient about the orgin of such messages is liable for the punishment of imprisonment upto 3 years with fine.
- **SECTION 66C** - Any person who dishonestly make use of the electronic identity such as signature or password of any other person, is liable for the punishment of imprisonment which may extend to 3 years with fine which may extend to rupees 1 lakh.
- **SECTION 66D** - Any person who by means of any communication device or computer resource cheats by personation is liable for the punishment of imprisonment which may extend to 3 years with fine which may extend to

[8] P. Oppili, First case to be prosecuted under IT Act, THE HINDU (Jan 05 , 2002), www.thehindu.com.

rupees 1 lakh.

- **SECTION 66 E** - Any person who intentionally or knowingly captures, publishes or transmittes the image of private area of any person without his or her consent is liable for the punishment of imprisonment which may extend to 3 years or 2 lakh rupees fine or with both.

- **SECTION 67** - Any person who publishes or transmits any obscene material in the electronic form is liable for the punishment which may extend to 3 years and with fine which may extend to 5 lakh rupees on first conviction and imprisonment which may extend to 5 years and with fine which may extend to 10 lakh rupees on second conviction.

- **SECTION 67A** - Any person who publishes or transmits any material which contains sexually explicit act in electronic form is liable for the punishment which may extend to 5 years and with fine which may extend to 10 lakh rupees on first conviction and imprisonment which may extend to 7 years and fine which may extend to 10 lakh rupees on second conviction.

- **SECTION 72** – Any person who illegally discloses any electronic information or other material which contains personal information of that person without the consent of that person to any other person is liable for the punishment of imprisonment which may extend to 3 years or with fine which may extend to 5 lakh rupees or with both.[10]

- **IPC SECTION 354C** – Any person who watches or captures the image or video of a women engaged in a private act (in circumstances in which she believes not being observed either by perpetrator or any other person) and disseminates such images or videos is liable for the punishment of 1 year imprisonment which may extend to 3 years with fine on first conviction and imprisonment of 3 years which may extend to 7 years with fine.

- **IPC SECTION 354D** – Any person who follows or attempts to contact a woman by the use of the internet or any other electronic communication commits the offence of stalking and is liable for the punishment of imprisonment which may extend to 3 years with fine on first conviction and imprisonment which extend to five years with fine on second conviction.

REASONS FOR THE GROWTH OF CYBERCRIME AGAINST WOMEN

The expansion of the technology is a positive aspect that can be regarded as an essential factor for the development of any country but simultaneously it is becoming the platform to escalate the crime rate with the advancement of technology against the weaker section of the society. The main victim of these crimes use to be women. The reasons for the increasing rates of these crimes are as follows:-

- Most of the cybercrimes remain unreported due to the hesitation and risk of social embarassment and social stigma.
- They do not take any intiative to report such crimes because of the fear of defamation of the victim and her family.
- Sometimes, the reason behind it is, the victim believes that she is the only person responsible for the crimes done to her.
- The patriarchical society existing in India, that encourages the victims to compromise to maintain peace and keep away the further disturbances in the family.
- There are no such specific laws recognised for the offences committed in the cyberworld against women.
- The National Crime Records Bureau (NCRB) does not maintain any separate records of the cybercrimes committed against females.
- There is a lack of awareness among the females of the society as to where to report such crimes.
- The judicial system of India is painfully slow, which is a major threat to the society as it does not provide justice at the proper time.
- Lack of vigilance from the part of the owner's of the websites to observe what is going on their sites.

MOTIVES BEHIND CYBERCRIMES AGAINST WOMEN

The motive behind any of the cybercrimes committed is the malafide intention of the cyber criminals who take use of the technology to carry out their plans. Some of the motives behind the cybercrimes against women are as follows:-

- Financial Profit – Alike so many offline crimes, the main motive of cybercrimes is to gain monetary profit. The cyber criminals usually demand money by threatening or blackmailing the victim to post their private pictures or videos captured by them with the use of different online identities.
- Sexual Motives – The weird sexual behaviour is illicit and it is considered harmful. Lots of people watch porn sites to fulfill their wrong desires and lust which impulses the cyber criminals to post on pornographic sites subsequently increasing cyber pornography.
- Entertainment Purposes – Unlike other cybercrimes, cybercrimes against women are done for the purpose of fun and entertainment by the use of internet.
- Emotional Motives – Internet is also misused by the cyber criminals outraged of anger because of love failure or someone who feels cheated to take revenge as the chance of their plans and tricks of being caught often gets reduced.

KEY FINDINGS

- Online abuse has become a serious issue in India, which affects more than half of the women as per the survey.
- 36% of the online harassment victims did not take any actions. 28% of them have reported that they have reduced their online presence after being abused.

- 30% of the online harassment victims who had experienced violence had found it extremely upsetting and 15% have faced serious mental issues like depression and insomia.
- The mechanisms on social media to report online abuse are inaffective and victims are more likely to block the abusers instead of reporting them.
- 30% of the victims have said about the unawareness of the laws to protect them from online harassments.
- 38% of the victims have characterized that the laws are "not at all helpful".[9]
- According to NCRB, the number of cases registered under the law has shown a decline of 46% in 5 years (2008-2012) and an increase of 156.7% in the year of 2012 under IPC and SLLs.
- A decline of 14.9% was registered in the same crime during 2015.
- In the year 2015, 40 cases were registered and it became 38 in 2016.
- The Indecent Representation of Women Prohibition Act, 1986 was 37.3% in 2016 has most of the cybercrimes against women were registered under IT Act, 2000.[10]
- About 27000+ cybercrimes were reported in the year 2017 with an averageof one every ten minutes.

SUGGESTIONS

- Don't share passwords with your trusted friend or partner as it is riskier to share passwords which may cause harm. Keep passwords secret and complex
- Don't share intimate messages or pictures to anyone, no matter how much trustworthy that person is. Be cautious as it may be unsafe and

[9] Japleen Pasricha, Cyber Violence Against Women In India – A Research Report, FEMINISM IN INDIA (Nov15, 2016), http://feminisminindia.com.
[10] Molly Ghosh, Introspecting the Gaps between Cyber Crimes against Women and Laws: A Study of West Bengal (Jan 17, 2018), https://itforchange.net.

sometimes can be used to harass you.

- Never go to meet the friend, you met online alone as it can be risky and may cause damage. Make sure to meet that person in a very populous place.
- Never accept friend requests from unknown person and don't feel weird in rejecting those friend requests on any of the social media.
- Block the people with whom you don't want to interact as safety comes first. In any point of time if you feel something fishy just block them immediately.
- If there is any cybercrime, go and report it instantly as the procedure for reporting cybercrimes is also somewhat similar as the reporting of any other offences.
- The law enforcement systems in India should be well equipped to deal with cybercrimes against women.
- The Indecent Representation of Women Prohibition Act, 1986 is the only gender specific act mentioned in the legislation. Some more gender specific act should be amended under the IT Act, 2000 to prohibit cybercrimes against women.
- The National Crime Records Bureau should maintain a separate record of the cyber crimes registered against women.

CONCLUSION

Over the past decades, the technology has become utterly an essential component of modern life. The dependency on the modern technology to support and facilitate our life has created more chances to misuse it resulting in the escalation of the cybercrimes mainly against women. Cybercrime against women in India is at its developing stage and growing at a large level very quickly.The cyber world provide an

enormous platform to cyber criminals to cause harm to the weakest section of the society. The Indian female netizens are still not aware about where to report the crimes. The female victims are not taking any intiative to report these cybercrimes or cyber abuse immediately. These kind of avoidance from the side of victims are giving more opportunity to the cyber criminals in the commission of more and more crimes in the cyber world. That is why women are easily targeted and victimized online.To avoid the cyber crimes, women should always be alert while using internet, social websites or having conversation with unknown person. Cybercrimes against women requires a comprehensive approach and need to be taken as severe violations like other offences committed against women. The government should organise more and more awareness programmes to educate the youth about the outcome of misusing internet and the prevailing cybercrimes against women presently. Apart from creating awareness, the government should develop more cyber cells for women. The investigating officers as well as judges should be trained specially to understand the cyber laws to provide justice to the victims. Laws under IT Act are insufficent and need to be amended from cyber specific to gender specific. The IPCs also should be amended and strict laws should be made to prohibit the cybercrimes against women. To eradicate cybercrimes against women, everyone needs to be sensitized about the misuse of internet which can result into various kinds of cybecrimes.