*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540*

# Study on the Case Laws Registered Regarding Cyber Crime against Women

**Shyamapada Ghorai[1]* Prof. (Dr.) N. K. Thapak[2]**

[1] Research Scholar, Swami Vivekananda University, Sagar, M.P.

[2] Associate Professor, Department of Law, Swami Vivekananda University, Sagar (M.P.)

***Abstract – The offices of computer technology have not turned out without downsides. In spite of the fact that it makes the life so quick and quick, however heaved under the shroud of threat from the deadliest sort of guiltiness named as 'Cyber crime' without computers, whole organizations and government tasks would nearly stop to work. The expanding reach of the internet, the quick spread of portable information, and the across the board utilization of social media, combined with the current pandemic of violence against women and girls (VAWG), has prompted the rise of cyber VAWG as a developing global issue with possibly huge monetary and societal results. The directly to internet utilization has now turned into a human ideal, as announced by the United Nations Human Rights Council in June 2016. Cyber-crimes use information technology and the internet as the essential methods for commission of illegal activities, which are restricted and deserving of criminal law of the land. While cyber-crimes might be carried out against persons, property and the government, this paper centers around cyber-crimes against women. In this research paper we studied about the Concept of Cyber crimes against Women, their categories, reasons leading to their Growth and the Case laws concerning it.***

***Keywords: Cyber, Crime, Women, Human Rights, Technology.***

----------X----------

## I. INTRODUCTION

The internet has two novel characteristics. Right off the bat, it rises above physical/topographical hindrances, and thus, the abuser might act from any piece of the world. Also, the internet stretches out secrecy to the clients. While this might be an ameliorating component for some clients, who can take cover behind the window ornament of obscurity even as they practice their entitlement to opportunity of articulation and assessment, it likewise bears secrecy to the abusers. Both the highlights present impressive difficulties in crime anticipation, crime detection and execution of the law (Wow Essay, 2009). To date, cyber VAWG has not been completely conceptualized or administered against at EU level. Besides, there has been no sex disaggregated EU-wide overview on the pervasiveness and damages of cyber VAWG and there is constrained national-level research inside EU Member States. In any case, the research that is accessible recommends that women are excessively the objectives of specific types of cyber violence contrasted with men. For instance, in a review of in excess of 9,000 German Internet clients matured 10 to 50 years, women were essentially more probable than men to have been victims of online sexual harassment and cyber stalking, and the impacts of these types of violence were increasingly awful for victims.

## II. CYBERCRIME

Cybercrime is a term used to comprehensively portray criminal activity in which computers or computer networks are a tool, an objective, or a position of criminal activity and incorporate everything from electronic breaking to refusal of administration attacks. It is likewise used to incorporate traditional crimes in which computers or networks are utilized to empower the unlawful activity. The Cyber crime can stop any railway where it will be, it might misinform the planes on its trip by misleading with wrong flags, it might make any imperative military data fall in the hands of outside nations, and it might end e-media and each system can crumple inside a fraction of seconds [2].

Women particularly young ladies unpracticed in cyber world, who have been recently acquainted with the internet and neglect to understand the indecencies of internet, and subsequently are most defenseless to falling into the trap of cyber crooks

and menaces, Cybercrimes and cyber tormenting is of different kinds (CAPEC, 2010), some are:

1. **Cyber Harassment:** Cyber Harassment is characteristic dreary conduct expected to exasperate or up rest a person however utilization of internet. A specific class of harassment which is sexual in nature is known as sexual harassment, among a few different things it significantly incorporates steady and undesirable sexual headway. Under Indian law sexual harassment has recently been characterized under the Criminal Law Amendment (Bill) 2013 as physical contact and advances including unwelcome and express sexual suggestions

2. **Cyber stalking:** Cyber Stalking fundamentally is conduct wherein an individual determinedly and over and over participates in a knowing course of bugging conduct coordinated at someone else which sensibly and truly cautions, torments, or threatens that person. This is a standout amongst the most discussed internet crimes in the advanced world. Cyber stalking includes following a person's developments over the Internet by posting messages (in some cases threatening) on the notice sheets frequented by the person in question, going into the visit rooms frequented by the person in question, always barraging the injured individual with emails and so forth. Cyber Stalking more often than not happens with women, who are stalked by men, or youngsters who are stalked by grown-up predators or pedophiles. Cyber stalkers target and disturb their victims through websites, talk rooms, dialog discussions, open distributing websites and email.

3. **Non-consensual Pornography:** Also known as cyber misuse or 'retribution pornography', non-consensual pornography includes the online dispersion of sexually realistic photos or recordings without the assent of the person in the pictures. The culprit is regularly an ex-accomplice who gets pictures or recordings over the span of an earlier relationship, and plans to openly disgrace and embarrass the person in question, in countering for closure a relationship. Notwithstanding, culprits are not really accomplices or ex-accomplices and the rationale isn't generally vindicate. Pictures can likewise be gotten by hacking into the injured individual's computer, social media accounts or telephone, and can mean to deliver genuine harm on the objective's 'genuine world' life, (for example, getting them terminated from their activity).

Once in a while viruses are covered up in apparently real emails and notice on web, which if once clicked contaminates the computer and because of this the person can't utilize their computers. The expanding reach of computers and the internet has made it less demanding for individuals to stay in contact crosswise over long separations. Be that as it may, the implications that empower the free stream of information and thoughts over long separations likewise offer ascent to a worryingly high frequency of flighty behavior. The helplessness and security of women is one of the greatest worries of any criminal and penal law, however lamentably women are still unprotected in cyber space. Cybercrime against women is on at disturbing stage and it might act like a noteworthy threat to the security of a person overall. The World Wide Web enables clients to flow content as content, pictures, recordings and sound. As of late, there have been various reports of women accepting spontaneous emails which frequently contain profane and unpalatable language. And the fundamental concern is that these issues are commonly not revealed by women (Oracle, 2003).

### 2.1 Cyber Crime Categories

**Data Crime:** An attacker screens data streams to or from an objective so as to assemble information. This attack might be attempted to assemble information to help a later attack or the data gathered might be the ultimate objective of the attack. This attack for the most part includes sniffing network traffic, yet may incorporate watching different kinds of data streams, for example, radio. In many assortments of this attack, the attacker is aloof and just watches ordinary correspondence, anyway in a few variations the attacker may endeavor to start the foundation of a data stream or impact the idea of the data transmitted. In any case, in all variations of this attack, and recognizing this attack from other data collection methods, the attacker isn't the planned beneficiary of the data stream. Not at all like some other data spillage attacks, the attacker is watching unequivocal data channels (for example network traffic) and perusing the substance. This contrasts from attacks that gather increasingly subjective information, for example, correspondence volume, not expressly conveyed by means of a data stream.

**Data Modification**: Privacy of correspondences is basic to guarantee that data can't be changed or saw in travel. Circulated conditions carry with them the likelihood that a malevolent outsider can execute a computer crime by altering data as it moves between locales. In a data modification attack, an unapproved party on the network intercepts data in travel and changes parts of that data previously re-transmitting it. A case of this is changing the dollar measure of a managing an account transaction from $100 to $10,000. In a replay attack, a whole arrangement of legitimate data is over and over interjected onto the network. A model is rehashing, one thousand times, a substantial $100 financial balance exchange transaction.

**Data Theft:** Term used to depict when information is illegally replicated or taken from a business or other person. Ordinarily, this information is client information, for example, passwords, social security numbers, Visa information, other personal information, or other private corporate information. Since this information is illegally acquired, when the person who stole this information is captured, it is likely the individual in question will be arraigned without bounds degree of the law.

**Network Crime:** Network Interferences Network Interfering with the working of a computer Network by contributing, transmitting, harming, erasing, falling apart, modifying or stifling Network data (Shantosh Rout, 2008)

**Network Sabotage:** 'Network Sabotage' or bumbling supervisors attempting to carry out the responsibilities of the general population they regularly are accountable for. It could be the above alone, or a blend of things. Be that as it may, in the event that Verizon is utilizing the assistance the youngsters, thwarting people on call line then they may blame network issues so as to inspire the government to intervene in the interest of open security. Obviously if the government powers these individuals back to work what is the motivation behind associations and strikes in any case.

## III. WOMEN IN INDIA

In Indian Society, it is stated that before lady involved an indispensable position and revered spot. Vedas celebrated lady as the mother, the maker and the person who gives life. The Vedic society revered her as a 'Devi' or 'Goddess'. In any case, her glorification was fairly legendary. Later in "Manu's Code", which is a cherished inheritance considered as deserving of being followed in India, a lady was esteemed to be a deep rooted ward, in the youth relying upon her father, in adulthood on her husband and in maturity on her child. Subsequently Indian women discovered her completely smothered and oppressed in a "Patriarchal Indian Society", which had confidence in sticking on to customary convictions prompting violence against women, either at the residential dimension or in people in general physically, candidly and rationally. At present, however women in India, comprise almost about portion of its populace and the vast majority of them are being pulverized under socio-cultural and religious strictures, one gender i.e., male gender alone has been controlling the space of India's social, financial, political and religious textures. It is extremely miserable to take note of that this patriarchal reasoning and doling out traditional jobs on women for being conceived as females, proceeds even today in the attitude of the general population and through them the society. The Constitution of India, in the journey for giving "Equality and Liberty" to all persons including women, attempts to advance "gender equality" through the Union Parliament and State Legislatures, Article 15 (3) of the Constitution enables the Union just as State Legislatures to protect and advance the interests of women by method for positive segregation, However, measurements demonstrate that females are the favored focus of wrongdoers and gender related crimes proceed unabated in spite of all gender protective social laws [6].

There are different types of crimes against women. Some of the time it is even before birth, on occasion amid the birth, commonly amid their adulthood and occasionally notwithstanding amid the fag end of their life, Violence against women both inside and outside their homes is a vital issue in the contemporary Indian society. In spite of the fact that crimes against women are proceeding, there is by all accounts changing patterns in such crimes, presumably because of the development of the majority rule system in India and International Treaties and Conventions, which force state gatherings to verify and protect the interest of women. The present investigation looks at the nearness of Changing Trends of Crimes against Women in India, in the period of Liberalization, Privatization and Globalization (LPG), i.e., the new financial arrangement received globally, especially in India in 1991.

## IV. CYBER CRIME AGAINST WOMEN

Cybercrime against women is on at disturbing stage and it might act like a noteworthy threat to the security of a person all in all. In India the expression "cybercrime against women" incorporates sexual crimes and sexual abuses on the internet. India is considered as one of the not many nations to enact IT Act 2000 to battle cybercrimes; This Act widely covers the business and financial crimes which is obvious from the prelude of the IT Act. The vast majority of the arguments identified with cyber crime against women answered to the police comes extremely close to Section 67 (Publishing or transmitting profane material in electronic structure) of the Information Technology Act 2000 that is particularly obvious from the accompanying contextual analysis.

In India Cyber harassments and offenses against women are thoroughly secured by the Protection of Harassment Act. The act is viewed as increasingly moderate to control gender driven Cyber harassment aside from those which include physical damages. Harassment through messages and Cyber-stalking might be viewed as a portion of the fundamental offenses against women in cyberspace. Hacking related activities may not generally be confined to crimes perpetrated against the country or the corporate substances alone however some time it might be viewed as a crime when done to put away computer data or the computer as a machine of any

female unfortunate casualty. To get to her personal information including pictures without legitimate approval, with aim to abuse it, convey it in the internet, adjust the substance and give a bogus impression of the victims and so forth, are additionally criminal activities like stalking or bullying (Prasun Sonwalkar, 2009).

### 4.1 Cyber Crime against Women: Reason leading to its Growth

The transcendental jurisdiction of Internet makes the significant threat the society as cybercrime. The primary casualty of this transgression can be viewed as women and kids. The investigation demonstrates that we have 52 million active internet clients in India which came to at 71 million in the year 2009. Among them working women net clients are 8 percent and 7 percent nonworking women in the year 2009 and 37 percent utilization of all clients getting to internet through cyber bistro. It is regular phenomenon that the critical information of the net surfer is being unveiled effectively by the proprietors of cyber bistro and then it is utilized for illegal purposes. In spite of the fact that colleague with technology is certain angle that can be viewed as critical for the improvement of any nation and yet it is turning into the source to expand the crime rate with technology against the more fragile section of the society, the explanation behind the expanding cyber crime rate against women can be sorted into two folds; legal and sociological reasons.

- **Sociological Reasons:** Most of the cyber crimes stay unreported because of the wavering and timidity of the person in question and her dread of defamation of family's name. Ordinarily she trusts that she herself is in charge of the crime done to her. The women are progressively helpless to the risk of cyber crime as the culprit's personality stays anonymous and he may continually threaten and shakedown the unfortunate casualty with various names and characters. Women still don't go to the police to gripe against sexual harassment, regardless of whether it is in reality or the virtual world they like to avoid off the issue as they feel that it might irritate their family life [8].

- **Legal Reasons:** The object of the IT Act is completely clear from its introduction which demonstrates that it was made for the most part to upgrade internet business consequently it covers business or budgetary crimes for example hacking, misrepresentation, and break of secrecy and so on however the drafters were uninformed about the security of net clients. Cyber defamation, email ridiculing, cyber sex, hacking and trespassing into one's privacy is space is regular now days however IT Act isn't explicitly referencing them under explicit Sections or arrangements. While IPC, Criminal Procedure Code and Indian Constitution give uncommon protection to women and kids for example unobtrusiveness of women is protected under Section 506 and rape, strong marriage, seizing and premature birth against the desire of the lady are offenses and indicted under IPC. Indian constitution ensures rise to directly to live, training, wellbeing, sustenance and work to women. In any case, a similar humility of women appears not to be protected when all is said in done with the exception of Section 67 which covers cyber-sex in Toto.

## V. CASE LAWS ON CYBER CRIMES AGAINST WOMEN

1. **Ritu Kohli Case:** Ritu Kohli Case was India's first case of cyber stalking, in this case Mrs. Ritu Kohli griped to police against a person, who was utilizing her personality to visit over the Internet at the website http://www.micro.com/, for the most part in Delhi channel for four sequential days. Mrs. Kohli further whined that the person was visiting on the Net, utilizing her name and giving her address and was talking vulgar language. A similar person was likewise purposely giving her telephone number to different gabs urging them to call Ritu Kohli at include hours. Subsequently, Mrs. Kohli got right around 40 brings in three days generally on include hours. The said call made a destruction in personal existence of the complainant thusly IP addresses was followed and police researched the whole issue and eventually captured the guilty party. A case was enrolled under the section 509, of IPC and from that point he was discharged on safeguard. This is first time when a case of cyber stalking was accounted for. Like the case of email harassment, Cyber stalking isn't secured by the current cyber laws in India. It is secured just under the ambit of Section 72 of the IT Act that culprit can be reserved remotely for rupture of classification and privacy. The charged may likewise be reserved under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again to shock the humility of women (PTI Contents, 2009).

2. One case was accounted for from Kottayam in Kerala where a girl went to meet with a person she had progressed toward becoming companion on Facebook. Anyway when she met him, she was snatched. The girl was anyway followed and later she told the police that when she met with the kid he had persuasively taken her to an inn and attacked her

3. **State of Tamil Nadu v. Suhas Katti:** In this case the denounced Katti posted foul, slanderous messages about a separated from lady in the yahoo message gathering and publicized her as a request for sex. This case is considered as one of the main cases to be reserved under the Information Technology Act, 2000 (IT Act). He was indicted under section 469, 509 of Indian Penal Code (IPC) and 67 of the IT Act 2000 and was rebuffed for a long time thorough detainment and fine. Previously mentioned cases were viewed as first time under its ambit Act. Aside from these cases there are couple of essential cybercrimes that fundamentally happens to the Indian women in the cyberspace, for example, harassment by means of email, cyber-stalking, cyber defamation, transforming, email ridiculing, hacking, cyber pornography and cyber sexual defamation, cyber being a tease and cyber bullying.

4. **Dr. L. Prakash v. Superintendent**: In this case the blamed was an orthopedic specialist constrained women to perform sexual acts and later on transfer and deal these recordings as grown-up stimulation materials worldwide. He was 3 (2008) 3 MLJ (Crl) 578 charged under section 506 (section II of the section which endorses discipline for criminal terrorizing to cause death or unfortunate hurt), 367 (which manages grabbing or kidnapping for causing death or appalling hurt) and 120-B (criminal intrigue) of the IPC and Section 67 of Information Technology Act, 2000 (which managed indecent distribution in the internet). He was condemned forever detainment and a monetary fine of Rupees 1, 25,000 under the Immoral Trafficking (Prevention) Act, 1956 (Vishwanath Paranjape, 2008).

## VI. CONCLUSION

In the course of the most recent three decades, computer technology has turned into an altogether universal part of present day life. The expanding reliance on technology to help and deal with our lives has made unparalleled open doors for crime and abuse. In fact, most types of crime presently includes technology somehow or another, regardless of whether using mobile phones and instant messages or increasingly novel uses of technology to carry out crimes that are not generally conceivable outside of computerized gadgets. Cyber space offers a plenty of chances for cyber criminals to make hurt blameless individuals. Indian women netizens are as yet not open to quickly report the cyber abuse or cyber crime. The most serious issue of cyber crime lies in the usual way of doing things and the thought process of the cyber criminal. Cyber space is a travel space for some, individuals, including guilty parties. While individuals don't live in cyber space, they travel every which way like some other spot. This nature gives the guilty parties the opportunity to escape after the commission of cyber crime. Numerous websites and blogs give security tips to the wellbeing of women and kids in the net. Yet at the same time then cyber crime against women is on rise. As they are the obvious objective and they can be victimized effectively for example why women are made the fundamental target. Subsequently, to counter cybercrime against women in India, stricter penal changes are required as well as an adjustment in training system is a colossal prerequisite. Such change can't emerge out of inside a solitary square of society yet individuals, government and NGOs and so forth need to cooperate to deliver such changes.

## REFERENCES

1. Wow Essay (2009). Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.

2. Crime in the Digital Age by Peter Grabosky and Russell Smith, Sydney: Federation Press, 1998

3. CAPEC (2010). CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

4. Oracle (2003). Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012

5. Shantosh Rout (2008). Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012

6. By Jessica Stanicon (2009). Available at: http://www.dynamicbusiness.com/articles/articles-news/one-infive-victims-of-cybercrime3907.html, Visited: 28/01/2012.

7. Prasun Sonwalkar (2009). India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html, Visited: 10/31/09

8. India emerging as major cyber-crime centre (2009). Available at: http://wegathernews.com/ 203/indiaemerging-as-major-cyber-crime-centre/, Visited: 10/31/09

9. PTI Contents (2009). India: A major hub for cybercrime, Available at: http://business.rediff.com/ slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm, Visited: 28/01/2012.

10. Vishwanath Paranjape (2008). Legal dimensions of cybercrimes and preventive laws, Pg no.33, Central law Agency, Allahabad, edn,.1st, 2010, 3 MLJ (Crl) p. 578

**Corresponding Author**

**Shyamapada Ghorai***

Research Scholar, Swami Vivekananda University, Sagar, M.P.