WOMEN AS A VICTIM AND SURVIVOR IN CYBERCRIMES

Written by ***Deepthy S***

B.A LLB, LLM (2013 - 2015) School of Indian Legal Thought, Kottayam, Kerala

ABSTRACT

With the advent of technology, cybercrime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Cybercrime against women in India is relatively a new concept. When India started her journey in the field of Information Technology, the priority was given to the protection of electronic commerce (e-commerce) and communications under Information Technology Act, 2000 whereas many crucial areas remained untouched. The Act turned out to be a half-baked law. Even though India is one of the very few countries to enact IT Act to combat cybercrimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the privacy and security of women in general is not covered fully by this Act.

Women victimization was recognised long back in the Post-Vedic times which still continue through today the forms of harassment have changed. The position of women has been vulnerable, always. Even if Equality is the key factor as far as a democratic country like India is concerned, there still exists and erupts new ways of suppressing her. And in the present era of technology, Hi- Tech forms of crimes are targeted against women through the use of internet, mobile phones and such type of electronic gadgets. The use of cyber space and its attendant features of anonymity continue to influence negatively the social and cultural aspects of society. While the cyberspace has provided secure tools and spaces where women can enjoy their freedom of expression, information and privacy of communication, the same benefits of anonymity and privacy also extend to those who do criminal activities of violence against women. The use of internet to stalk, abuse, intimidate, harass, and humiliate women is palpable.

So keeping in mind these facts the thesis entitled 'Women as a victim and survivor in cybercrimes' has been prepared with the inclusion of the many case laws and suggestions in the end for the protection of women from being tortured.

INTRODUCTION

"*Yatra naryastu pujyante ramante tatra Devata……yatraitaastu na pujyante sarvaastatrafalaah kriyaah*"

…….Manusmriti 3.56

which reads: - *"where Women are honored, divinity blossoms there, and where women are dishonored, all action no matter how noble remain unfruitful".* Literary evidence on ancient Indian culture suggests that kings and towns were destroyed because the rulers troubled a single woman. For example, Valmiki Ramayana teaches us that Ravana and his entire kingdom were wiped out because he abducted Sita. Veda Vyasa's Mahabharata teaches us that all the Kauravas were killed because they humiliated Draupadi in public. Elango Adigal's Sillapathigaram teaches us Madurai, the capital of the Pandyas was burnt because Pandyan Nedunchezhiyan mistakenly did harm to Kannaki.

So far as the Indian conceptions of woman as a mother are concerned, it was believed that there is no greater guru than mother." (*Mahabharata*, Shantiparva, 30.9). Our own life is a gift from our mother's life. We were nourished by her, we spent nine months in her womb, and her love sustained us. Through this means, before any child learns hatred or aggression, they first know the love of a mother who can instill the ways of forgiveness and kindness in the child. Scrutinizing the ancient Bharat culture, it is evident that the status and position attached to woman in every phase of her life, as an independent dignified personality, was at its zenith.

Respect for womanhood has been the most cherished value of society from times immemorial. As far as the status assigned to women in Bharat, the eminent English author Kerry Brown in her celebrated book 'Essential Teachings of Hinduism while answering the adverse comments made against the verse in Manu Smriti where it is said that at every stage of the life of a woman, it is the responsibility of males as father or husband or sons as the case may be, to protect her having regard to the fact that she is a woman. No answer or argument can be more forceful as made by

Kerry Brown at para 238 of her book thus:

> *"In Hinduism a woman is looked after not because she is inferior or incapable but, on the contrary, because she is treasured. She is the pride and power of the*

society. Just as the crown jewels should not be left unguarded, neither should a woman be left unprotected"

Womanhood has been reverenced in ancient Indian culture as a manifestation of divine qualities. Womanhood is the symbol of eternal virtues of humanity expressed in compassion and selfless love. Indian philosophers of yore (the *rishis*) considered that the seed of divinity grows and blossom in a truly cultured society where women are given due respect and equal opportunities of rise and dignity. The scriptures and later works on Indian culture and philosophy stand witness to the fact that women indeed received high recognition and respect during Vedic age. Vedic period can be best termed as the period of feminine glory, masculine sagacity and liberalism.

This did not last long and the later period of our society brought forth the deteriorated and declined position of women. Womanhood never gained any prominence or divinity in the latter part of our society. Concept of woman as a mother and sister were completely withered away. Respect of womanhood, which are practiced to be ingrained in the mind of every individual, especially in men found no place aftermath. They were merely over looked as an object of pleasure rather than a subject of dignity. The reasons for such radical changes were urbanization, industrialization and the sudden blow of technological era upon the lives. They were subjected to many forms of humiliation mentally and physically. And as a solution, much legislation was introduced to cope up with the issue. Still then complete eradication of the harassment could not find place as traditional offences are continued to be committed in a newly fashioned way with the assistance of technology. Such offences, even though unique in content, are furiously capable of harming the life, dignity, reputation of women and much wider in extend, magnitude and consequence.

Period of technology- In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of IT gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyze etc. with the use of high technology. Information and Communication Technology (ICT) is benefiting billions across the world by bridging certain gaps and multiplying human potential in every walk of life. Digital services provision that is being developed for our society has enormous positive potential. The internet has revolutionized

the way businesses approach and conduct work. For consumers, the idea of purchasing online is appealing for several reasons. A well designed and implemented e-commerce system can lower transaction costs, reduce inefficiencies, promote better information flow, and encourage better co-operation between buyers and sellers. With little more than a click of a mouse, business can communicate, engage in commerce, and expand their business opportunities. At the same time, there are certain social, political, and economic implications being observed globally either in the form of hacking activities or cybercrimes against women. Along with promoting the use of Information and Communication technologies since their inception, countries have been looking at ways to counteract the negatives simultaneously. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cybercrimes at the domestic and international level as well.

Cybercrimes unlike the traditional crimes are easy to be committed and the chances of detection are comparatively less as this technology knows no physical boundaries; it flows more easily around the world. Subsequently the criminals are increasingly located in places other than where their acts produce their effects and Cyberspace is no exception to it. Cyberspace is a new horizon controlled by machine for information and any criminal activity where computer or network is used as the source, tool or target is known Cybercrime. When Information Technology Act was introduced, its main aim was given for protection of electronic commerce (e-commerce) and communications under Information Technology Act, 2000 whereas cyber socializing communications has not been given much prominence.

In cyber space, women are subjected to harassment via e-mail, cyber-stalking, cyber defamation, morphing, hacking, cyber pornography, cyber flirting and bullying. One of the most common forms of it is depicting a woman through false and derogatory identities mostly through social networking sites. The typical nature of victimization includes the creation of fake profiles which may include picture(s) and personal information. Women are exposed to an audience in a fashion in which she never wish or authorize anyone to expose her. Cases of cyber victimization of women especially through offences like the creation of fake profiles to describe the victim indecently, leaves a deep impact on the victim. Not only does this indecent representation remain ‘alive’ for a long time to create

huge embarrassment for her, it also deters her professional as well as personal reputation. It is believed that Over 75% of its victims are females. The motives behind cyber stalking can be done mainly for sexual harassment, for obsession for love, for revenge and hate and for ego and power trips. The availability of free email and website space, as well as the anonymity provided by the chat rooms etc is culpable for it. The biggest problem of cybercrime lies in the modus operandi and the motive of the cyber criminal. Cyber space is a transit space for many people, including offenders, where they can come and go like any other place. This nature provides the offenders the chance to escape after the commission of cybercrime.

The ironical fact on the other side is that our women netizens are still not open to immediately report this crime. From personal to social constraints, the victim continues to suffer to avoid any embarrassment she or her family may face and this behavior gives offender an upper hand. This growing menace needs to be checked with girls taking a lead in speaking up with the help of their friends, family and police for no one has any right to defame you and intrude in your liberty and dignity, no matter what.

In this paper, the researcher mainly focuses on the women victims on cyber space mainly because of certain reason. They are:

(i) The unequal ratio of men and women victims of cybercrimes. Various studies and statistical analysis has pointed out that women are more prone to cyber-attack. Despite the fact that the harassers can be both men and women, in the year 2000, there were 87% women victims and among the harassers there were 68% men. In the year 2004, among 196 victims, 65.9% of the victims were women whereas 52.5% harassers were men. And this unequal ratio of men and women continues till date and the consistent high ratio of female victims and male harassers prove that women remained the most vulnerable targets for cybercrimes.

(ii) The difference in the impact of victimization between men and women. Unlike a women victim, a men victim are not subjected to gross humiliation by the society as a whole, he may neither be reduced as a ‘sex item’ like his female counterpart. His victimization may be judged from the perspective of economic losses. On the other hand, a women victim may be ostracized by the society. Unlike the male counterpart, she may not take the online harassment so easily. It may engulf her in

to the feeling of shame and hatred for herself. Sexuality still remains the biggest disadvantage for women in establishing equal rights.

(iii) The global approach towards the issue have not gained momentum. The concept of cybercrime against women has therefore become standstill within the meaning of obscenity, pornography and stalking to a certain extent. An analysis of the existing cyber legislation reveals that the drafters are not acquainted with the changed cyber culture so as to include the gender protective regulatory rules.

(iv) New trend of victimization of women in the cyber world are over shadowed by the traditional offences committed against women in the offline world. The existing vacuum in law so as to combat with the cybercrime instigated the growth of ongoing experiments with digital technologies to victimize women.

Thus, it could be deducted that the women victims need a faster restorative procedure to avoid further escalation of agony and trauma. Women deserve a different treatment from that of child victims and such other type of cyber offences. Thus, the research proposes to establish that women form a separate group of cyber victims.

CONCEPT OF CYBERCRIME

The internet has revolutionized the way the individual interacts with each other. The phenomenal growth of internet has provided new vista for computer crimes. A new strain of crime has developed through the invention of the computer and internet. The term cybercrime[1] is a misnomer which is not radically different from the concept of conventional crime**.** The concept of cybercrime is not new in the knowledge society of 21st century, the kind of which is more or less same since 1860. The new technology has facilitated the commission of old crime in a new-fashioned way as it is easy to be committed with little resources but damage caused could be very huge. Thus, a simple definition of cybercrime is any unlawful act where computer is either a tool or target or both**.**[2]

---

[1] The word 'cyber space' has been joined by 'William Gibson' in 1982 in his novelette '*Burning Chrome*' in Omni magazine and in his novel 'neuromancer'. The phenomenal growth of internet has provided new vista for computer crimes.

[2] Jyothi Rattan, *Cyber Laws & Information Technology*, Bharat Law House Pvt. Ltd., 3rd Edition, 2012, p. 210.

Definition:

- The Cambridge English dictionary defines cybercrime as crime committed with the use of computer or relating to computer, especially through internet.
- According to Pawan Duggal, cybercrime is any criminal activity that uses a computer either as an instrumentality, target or means for per perpetuating further crimes.[3]
- European Union (EU) defines cybercrime as criminal activities that specifically target a computer or network for damage or infiltration and also refers to the use of computers as a tool to conduct criminal activity.

Features:

1. Computer is essentially an element of cyber criminality and it is either a tool or target of cybercrime.
2. Cybercrime can be committed without any physical contact.
3. Anonymity is the basic feature in cybercrimes. Identity of the person using cyber space remains unknown.
4. Cybercrimes transverse jurisdictional boundaries. Presence of the offender is not required and crime can be committed from anywhere in the world with a mouse click.
5. Cybercrimes can be committed against any computer, computer system, information, individuals, government or any organisation.
6. Magnitude of the cybercrime is comparatively very high.

Classification of cybercrimes:

1. Computer related offence.
2. Content related offence.
3. Offence against confidentiality, integrity and availability of computer data and system.
4. Copyright related offence.

[3] Pavan Duggal, *Convergence on Cybercrime*//http// www.cyberlawindia.com//

Computer Related Offence:

This category covers a number of offences that need a computer system to commit such offences which include

- Computer related fraud:

  A variety of services are offered by the business to the consumers through internet. The e-business possible through internet has always found advertise in the form of fraudsters whose identity and location is not easy to trace. The fraudsters are using newsletters through which they provide free advice to the prospective investors recommending stocks where they should invest. Their recommendations are generally bogus and then cause loss to the investors.[4]

- Computer related forgery, phishing and identity theft

a. Computer related forgery means any alteration or change in e-document or creating false e-document is called as cyber forgery

b. Phishing is an illegal activity where by fraudulently sensitive information is acquired, such as password and credit card details, by a person misrepresenting himself as a trustworthy person or business in an apparently official electronic communication.[5]Communications purporting to be from popular social networking sites, auction sites, bank, online payment processor or IT administrator are commonly used to lure unsuspecting public. Attempts to deal with phishing include legislation, user training, public awareness, and technical security measures.[6]

c. Identity theft describes the criminal act of fraudulently obtain and using another person's identity. In general, the offence describes as identity theft contains 3 different phases:

   i. In the first, offender obtains identity related information.

   ii. Second phase is characterized by interaction with identity related information prior to the use of that information within criminal offence.

---

[4] Farooq Ahmed, *Cyber Law in India*, New Era Publications, 2nd Edition. 2005,P.341

[5] Ibid at p.217

[6] Phishing, http://en.wikipedia.org/22-12-2014 (last seen)

iii. Third phase is use of the identity related information ion criminal offence.[7]

Content Related Offence:

This category covers content that is considered as illegal like child pornography, libellous and defamatory materials etc.

- Cyber pornography and child pornography:

  It is considered as one of the serious crime over internet. It means publishing or transmitting of any obscene material in electronic form that is lascivious or appeals to the prurient interest. It also prohibits any material in electronic form that tends to deprave and corrupt persons who are likely to read, see or hear the matter embodied in it.[8] Child pornography is depicting children in such type of sexually explicit contents. Publication, distribution of such material is an offence under the IT Act, 2000.

- Libel and defamatory information:

  Cyber defamation: In general defamation means to lower down the reputation of another person without justification. When defamation takes place with the help of computers or internet, it is known as cyber defamation. Cyber defamation is an act, deed or words etc in cyber space to harm reputation of other person.[9]

  Internet can be used to spread misinformation just an easily as information. Websites can present false or defamatory information especially in the form of chat rooms, where user can post without verification of moderators.

- Spamming:

  It is the unsolicited bulk emails which pose as a nuisance at first instances, but proven to be a biggest problem. This receiving of unsolicited bulk emails is known as spamming. These spams are generally sent by commercial companies as ads of their products and services especially when they are cross posted to several news groups.[10]

---

[7] *Supra* Note 4
[8] *Supra* Note 2 at p.219

[9] *Ibid*
[10] *Supra* Note 2 at p. 223

Offences Against Confidentiality, Integrity And Availability Of Computer Data And Systems:

Offences under this category are directed against 3 legal principles confidentiality, integrity and availability. Unlike crimes that have been covered by criminal law for centuries, the computerization of offence is a recent phenomenon.

- Illegal or unauthorized access:

  Any one secures access to the computer without the permission of the owner or person in charge is said to have committed illegal access.[11] This includes hacking. It is the intentional breaking in to the computer resources. Hacking can be of many types, depending upon the objective. Financial hacking - which are done to cause financial loss to competitors or win the confidence of client.

  Secondly, recreational hacking where it is done for pleasure and hacker attempts to prove his ability without doing any damage to another person. Thirdly, Intelligence hacking – done to infringe the creative work of another person. Finally, grudge or military hacking which is done with a grievance against some person or organization or against state.[12]

- Password cracking, another type of illegal access.:

  Most widely known security measure is password. It is used to prevent unauthorised access by anyone other than the owner. During login session, systems cache password in memory which makes the system vulnerable to hackers. A program called crack helps in finding all user account whose password where chosen from the dictionary.[13]

- Data espionage:

  Espionage or, casually, spying involves a spy ring, government, company/firm or individual obtaining information considered secret or confidential without the permission of the holder of the information.[14] Sensitive information is stored in computer system. If the computer is connected to internet offenders can try to access this information via the internet from any place in the world. The value of sensitive information and the ability to

[11] *Supra* Note 4

[12] *Ibid*

[13] *Supra* Note 5 at 310-312

[14] Available at http//www.wikipedia.com// (last accessed on 22-12-2014)

access it remotely makes data espionage highly interesting. Spying is very important for government and business entities to know about the product and market strategy of their rivals. Electronic media has provided new opportunities to have such information by spying.[15]

- Data interference:

  Computer data are vital for private users, business and administration all of which depends upon the integrity and availability of data. Lack of access to data can result in considerable damage. Offenders can violate the integrity of data and interferes with them by-

  i. Deleting data or;
  ii. Suppressing data or;
  iii. Altering data or;
  iv. Restricting access to them

- System Interference:

  The same concern over attack against computer data applies to attack against computer system. System interference can be made possible by way of cracking and hacking and also by the introduction of computer worm and viruses.[16]

- Viruses:

  A computer virus is a malware program that, when executed, replicates by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts.[17] Anyone without the permission of real owner or person in charge of computer introduces or causes to be introduced any computer contaminants or virus is liable. Computer virus means any computer program, instruction or data that destroy, degrade damage or affect the

[15] *Supra* Note 10 at 223

[16] *Ibid*

[17] *Supra* Note 14

performance of computer resources or normal working pattern of the computer. Sole object of inserting virus is to corrupt data on the computer system and can cause large loss to the person in charge.

Copy Right and Trademark Related Offence:

One of the vital functions of the internet is the dissemination of information. Companies use the information about their product and services. Their brand image and corporate design may be used for the marketing of counterfeit products with counterfeiting copying logos as well as product and trying to register the domain related to that particular company.

- Copyright Infringement:
  Offender violates the copyright of author by using computer resources. with the switch from analogue to digital, it enabled the entertainment industry to add features and services to movies on CD's/DVD's and have proved more sustainable than records. The basis of copyright violation is fast and accurate reproduction. It is possible to duplicate digital sources without loss of quality and makes as many copies from it. One of the biggest difficulty with technology is the copyright protection technology can be circumvented. Offenders have developed software tools that enable the user to make copy protected files over the internet, free of charge.

- Trademark Related Offence:
  Trademark violation is a common term in conventional crimes. With the advancement in technology, the same has been carried out in digital world too, which makes the violation much easier in sophisticated ways. The serious offences include use of trademark in criminal activity and domain name related offences. Good reputation of the company is often linked with its trademark. Offenders use brand name fraudulently in number of activities including phishing, where millions of emails are sent out to internet uses assembling enables from legitimate companies.
  Another issue is cyber squatting which describes the illegal process of registering a domain name identical or similar to a trademark of a company. More often, offenders seek to sell the domain name for high price to the company and mislead users through their supposed connection to trademark.

INFORMATION TECHNOLOGY ACT, 2000

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology **"INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000]** was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes. The above Act was further amended in the form of **IT Amendment Act, 2008 [ITAA-2008]**.

The ITA-2000 defines 'Computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. [18]The word 'computer' and 'computer system' have been so widely defined and interpreted to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.[19]

Objectives of I.T. legislation in India:

> *"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian*

[18] *Cyber Laws in India*//http://www.iibf.org.in/ 22-12-2015 (last seen)

[19]Article by Rohit K. Gupta, *India: An Overview Of Cyber Laws vs. Cybercrimes: In Indian Perspective,* 12 August 2013, http://www.mondaq.com/

Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000. The Act essentially deals with the following issues:

(A) Legal Recognition of Electronic Documents
(B) Legal Recognition of Digital Signatures
(C) Offenses and Contraventions
(D) Justice Dispensation Systems for cybercrimes.[20]

Information Technology (Amendment) Act, 2008

Major change that has been incorporated by the amendment Act, 2008 are as follows:-

i. The term 'digital signature' has been replaced with 'electronic signature' to make the Act more technology neutral.

ii. A new sec. has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.

iii. A new sec. has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.

iv. A new definition has been inserted for intermediary

v. A new sec. 10A has been inserted to the effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.

vi. The damages of Rs. One Crore prescribed under sec. 43 of the earlier Act of 2000 for damage to computer, computer system etc. has been deleted and the relevant parts of the section have been substituted by the words, 'he shall be liable to pay damages by way of compensation to the person so affected'.

vii. A new s. 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such

[20] Supra Note 18

body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected.

viii. S. 66A to 66F have been added to Sec. 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism,[21]whereby S66A got repealed by SC.

ix. S. 67 of the IT Act, 2000 has been amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Rs.100, 000 to Rs. 500,000. Sec. 67A to 67C have also been inserted. While S. 67A and B deals with penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Sec. 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

x. In view of the increasing threat of terrorism in the country, the new amendments include an amended s. 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, s. 69A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

xi. S. 79 of the Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if;

(a) The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; [22]

---

[21] *Ibid*

[22] Available at http://www.indiancybersecurity.com/ (last accessed on 22-12-2014)

(b) The intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission;

(c) The intermediary observes due diligence while discharging his duties. However, sec. 79 will not apply to an intermediary if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act or upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

xii. A proviso has been added to Sec. 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957. [23]

The major Acts, which got amended after enactment of ITA

The Indian Penal Code, 1860

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under sec. 463,464, 468 and 469 read with the ITA/ITAA under S. 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

[23] *Ibid*

The Indian Evidence Act 1872

Prior to enactment of ITA, all evidences in a court were in the physical form only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as "all documents including electronic records" were substituted. Other words e.g. 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were also inserted to make them part of the evidentiary importance under the Act. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in S. 65B of the Act.

The Bankers' Books Evidence (BBE) Act 1891:

Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as: "'bankers ' books' include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data ...to retrieve data that is lost due to systemic failure or ....

The above amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

This is an overview about the concept of cybercrime and its various forms**.** At present, threats in the field of cyber space are tackled by way of 1T Act, 2000 which received

prominence by 2008 Amendment Act. By the total analysis of the whole act, further modification is very important so as to include the left out portion as to woman and children which is in question.

VICTIMIZATION OF WOMEN

Technological developments related to communication have developed a communion among the people, who lives world apart. The internet is one of the greatest inventions in the arena of communication. With the advent of internet, the whole world has become a global village. It has created a virtual world with no boundaries, which gives people ample opportunities to ameliorate both personal and professional relationships across borders. The socio economic and cultural fact of life has been tremendously affected owing to the rise of globalization. The cyber space has been a blessing to human civilization. Internet has connected people around the globe. The desire to know what is unknown is indispensible of human nature.

One of the benefits which internet has provided to every section of the society is empowerment, including woman. The social networking websites have developed a new arena for socializing. Irrespective of any distinction, Women in the society are exulting with this liberation to the fullest. From online shopping to net banking, from e-tickets to e-tax filing, it has made the life of people easy. It has enabled women to fight for equality even within the confines of their society. They can now share their experience to the whole world and this advantage of being able to share their success stories as well as their problems have given them a platform in the global world. Most woman users avoid this new way of socialization as a stress relieve. Along with providing them a platform to voice their struggles and success of life, it inscribes new spaces of power, which is accompanied with knowledge.[24]

Ironically on the one side the internet is serving as a boon, but on the other side it has made the life of the women insecure due to rising cybercrime in the virtual world. Women of all the ages and milieu are in jeopardy with the coming up of internet. Few researches have established the

[24] Tanaya Saha & Akancha Srivastava, Article ;- *Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization*, International Journal of Cyber Criminology, Volume 8 Issue 1 January - June 2014

internet as the most chosen mode of the offenders to harass and victimize women. The foremost aim of such sorts of victimization remains the same as that of pre-internet era i.e., damaging the reputation of the woman victim and creating fear factor in the victims' mind. The behavioural factors that contribute to such victimization may include broken relationships, ex-partner harassment, professional rivalry, male dominance and chauvinism, sudden exposure to digital technologies and even for monetary gains.[25]

Victimization may begin by numerous methods such as, either befriending the victim with original name but portrayed as a 'Good Samaritan' or winning her trust under a camouflaged identity or shadowing her cyber activities or encouraging others to add to the ongoing victimization process of the victim. Cyber technology has become a prime tool to carry out such victimization in an almost successful manner due to digital ways and similarly, cyber space has proved the biggest platform to harass women in a most cruel way as the victimization can be viewed by millions of digital audience emails, public and private chat rooms, search engines, social networking sites and websites along with various digital technologies are the chosen modes of many offenders who victimize innocent women. There could be three factors for offenders choosing these unique methods for victimizing women.

1. It successfully generates instant fear and trauma in the minds of the victims.
2. The perpetrator is omnipresent, yet no one can find him out and prevent his atrocious activities.
3. Ones the electronics devices through which there communications were access by shrewd perpetrators are destroyed, it becomes really hard for the victim as well as the govt. reporting agencies like the police to nab him.[26]

MODE OF VICTIMIZATION – a statistical study

Cyber era can be separated into three period depending upon the usage of cyber communications. They are-

[25] Halder, D., & Jaishankar K., Article on *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations.* (June, 2011) Hershey, PA, USA: IGI Global. ISBN: 978-1-60960-830-9 (E-Book)

[26] Ibid

- E-mail Period (since 1990's) when emails were the only ways of digital communications and no strong universally accepted regulations other than EU Conventions on cybercrime 2001, ruled the cyber world.
- Chat Room Period (begun in late 1990's and early 2000) after the digital communication saw a boom through email period, came the public and private chat room period, whereby people could exchange their personal information.
- Cyber Social Networking Period (began in early 2000): In 1997, social networking websites were launched in US. The concept became immediately popular among other entrepreneurs, internet users and numerous social networking sites were born in the US in, & around 2000 – 2001. This period also saw booms in social interactions through blogs, adult dating sites, online bulletin boards etc.[27]

It has been seen that with each of these periods, new methods have been adopted by the perpetrators to victimize innocent women on the internet. The statistical resource of WHOA[28] shows that in the year 2000, 87% victims were female and the highest chosen mode of victimization was through emails.

The 2006 WHOA statistics shows that 70% of female victims and 31% of the victimization had been carried out through emails, 17% through instant messaging, 16.5% through message boards including forums, groups and user nets etc and nearly 7.5% of the victimizations had been done through chat etc. WHOA also reported 5% victimization through social networking sites and 1.5% victimization had been done through dating sites in 2006. In 2010, there were 73% female victims by way of emails, instant message, social networking sites, blog, Skype, gaming sites, Craig list, dating sites etc were used to victimize.[29]

FACTORS

There are various factors which instigate crime against women to grow. These are as follows:

---

[27] *Ibid*

[28] Working to Halt Online Abuse (WHOA). (2008). Cyber stalking statistics. Retrieved on 28th April, 2010, from http://www.haltabuse.org/resources/ stats/2008Statistics.pdf

[29] *Supra* Note 2

a) Patriarchal approach of the law and justice machinery of most of the cyber savvy nations towards this grave issue.
b) Cries of the women victims of crimes of the internet are often ignored as such and crimes do not fall in the category either economic crime or crime against state or crime against children.
c) Bullying or teasing a woman in open web space never attack any law enforcement intervention as the female victim in expected to be matured enough to handle the situation as an adult.
d) Unless the victim is established the fact that her rights have been infringed (which in majority of cases is extremely painful traumatizing for the victim), the law guarding the freedom of speech and expression of the individuals will remain as a silent motivator for enhancing the defamation of the victim.

India is predominantly a patriarchal and orthodox country and women who are victimized are mostly blamed and online victims are no exception. There are instances where marriages of woman were broke down due to online victimization. Also there is less legal protection to them compared to their western counterparts and the Indian women victims do not get adequate solutions for their victimization from the ISP's governed predominantly from a western cultural perspective.[30]

CYBER SOCIALIZATION

Socialization through internet, mainly social networking Websites (SNW) has become a favourite hobby for self supporting, educated, independent modern women of 21st century. It helps users to make new 'virtual friends' and offer 'promise' to reunite with old friends and relatives. Most women users avail this new way of socialization as a stress reliever. [31]

Cyber Socialization can be defined as the "computerised interaction with known and unknown individuals for the purpose of research, entertainment, establishment of friendship or

[30] *Supra* Note 1

[31] Debarati Halder and Karuppannan Jaishankar, Article on *Cyber Socializing and Victimization of Women*, September 2009, str. 5-26 ISSN: 1450-6637 DOI: 10.2298/TEM0903005H

relationships due to feeling of loneliness, or sexual gratification." Internet socialization is 'electronic interaction with virtual friends through chat rooms, emails, forums and social networking sites.'

Even though social networking websites have opened a wide window for socializing, they have also opened flood gate for various crimes against women in the cyber space. It is unfortunate that even though European Union (EU) conventions on cybercrimes established strict rules to control content related offences child pornography and identity theft related offences for securing e-commerce have proliferated. The draftsman of EU convention never considered victimization of women in the cyber space as a big issue like child pornography or hacking. Women victims therefore remained as a secondary concern for all developed cyber savvy nations. This lacuna reflects very much in the growing crime incidents targeting women in cyber space.[32]

The 10th UN congress on prevention of crimes and treatment of offenders, which was held in Vienna in 2000 made the first move towards recognizing the universal need for preventive measures against cybercrimes. The declaration of Vienna regarding cybercrime preventive measures was well developed in Council of Europe's Convention on Cybercrime, held in Budapest, 2001. Even though several cyber offences were defined from criminological perspective as early as in 70's and 80's, it was only after the EU convention on cybercrime (2001), that there offences were universally criminalized. However, resolutions of the conventions were mainly drafted to protect the e-commerce and not to prevent attack on human privacy and dignity. By cyber victimization of ordinary citizens had already started getting its momentum since 2000 and it was rapidly rising due to easy access to personal information of women in target, easy way to communicate through social networking sites and absence of proper preventive legal measures.[33]

[32] *Ibid*
[33] *Ibid*

TYPOLOGY & PATTERN OF VICTIMISATION

Women are victimized in different patterns by the abusers who can be an individual or even a group of individuals. The victimization type differs on the basis of various factors. For example, on the basis of the victim's sexuality, her ideologies, her marital status, her profession, professional commitments, the regularity of her participation in some chosen groups etc. Again the abuser can be both male and female. Similarly, the offences can be either sexual or non-sexual in nature.

In most cases, male harassers attack the victim for sexual purposes like morphing, using the image for pornographic purposes, cyber stalking etc and non sexual purposes such as harassment and bullying. Female perpetrators however, victimize women mainly for ideological differences, hatred or for taking revenge. Such attacks may not be sexual in nature.

Based on the above criteria, the typology of the offences against women victims are as follows:-

a) Cyber verbal abuse by groups of perpetrators expressing hatred: It can be called as a 'cyber mob attack' where a female member may be attacked by group of perpetrators both in the community wall and also message boards of social networking sites.
b) Cyber Defamation: Cyber tort including libel defamation is another common crime against women in the net. This occurs when defamation takes place with the help of computers or internet. eg:-emotional breakup may lead the male member to spread lies about a female member to others by way of messages or posts.
c) Cyber Stalking: It involves following a person's movement across the internet, by posting messages bulletin boards frequently by the victim, entering chat room frequented by the victim etc.
d) Morphing: Morphing is editing the original picture by unauthorised user or fake identity. It was identified that females picture are downloaded by fake users and again uploaded on different websites by creating fake profiles after editing it.
e) Cloning: Cloned/fake profiles of female victims are created by stealing the personal information of the female members. The cloned profile presents the original profile in such a manner that people are duped.
f) Cyber Pornography: Sexually explicit depiction of persons in word or images created with primary, proximity aim and reasonable hope of eliciting significant sexual arousal on the

part of consumer. It include pornographic website, magazine produced using computers and internet.[34]

g) Hacking: Unauthorized or illegal access. Particular targets are chosen and their profiles are hacked. Their personal information may be used for evil purposes.[35]

h) Cyber Harassment: it is not a new concept. It is similar to harassment in real world and the only different is the medium.ie, computers and internets. Harassment including blackmailing, threatening via messages or emails.

i) Cyber Bullying and Name Calling: The use of electronic communication to bully a person, by sending messages of intimidating or threatening nature. Objective may be hatred or frustration or to make simple fun off.[36]

REASON FOR THE GROWTH OF VICTIMISATION

- Easy availability of victims (women's) personal information

  Social Networking Sites are made to set other people know the existence of the profile owner. Hence users give away their vital information like residential address, marital status, age, phone number likes and dislikes etc even though many social networking sites provide options for using pseudo names and publication of such information as only 'optional' many 1st time registrants, including women, float their personal information in the web through these social networking sites without actual knowing the dangerous effect of it. This gives a huge opportunity for harassers to victimize the targets.[37]

- Ignorance and negligence of the users

  Several factors which push women to become victims in the social networking sites, the ignorance of the policy guidelines and safety measures stands first. The social networking sites presently give wide options to protect oneself from being harassed in various modes like setting up security measures, "locking" personal albums and message boards, blocking the harasser, preventing aliens from one's personal information, preventing unknown

[34] *Ibid*
[35] *Ibid*
[36] *Supra* Note 8
[37] *Ibid*

persons from writing in ones message board, blocking and banning individuals from community and groups and hiding ones profile from the internet. Majority of the women join the social networking sites without checking any of such safety measures.

Maximum of the respondents have never read policy guidelines before registering with the social networking sites, many of them have checked availability, safety-tips only after victimized themselves or have heard of their friends experiences. A majority of them have turned on their security button and 'locked' their albums and message book only after they had experienced some sort of harassment.[38]

- Lackadaisical response of the Social Networking Sites

  In most cases cyber socializing becomes dangerous due to nonchalant response of the social networking sites. Most of the social networking sites have an option to report any abuse of their services. But in most cases, social networking sites have their own policies to treat the post as defamatory or harassing but the stipulated time for taking action within may vary from 24 hours to 15 days. Impact of offence may be so that the victim needs to take action within 24 hours. The victim either has to withdraw herself from the 'societies' she is member of or she has to cancel her entire profile to wave off all the hazards. The delayed response or even nil response from the website authorities increase the panic in the victim and the harasser gets infinite opportunities to harm the stipulated time.[39]

- Globalization, Women's Identity Crisis And Emotional Exploitation: Psychological Reason

  With the rise of urbanization and globalization process, the Indian family structure has changed. Traditionally, joint family system existed in India. However, migration from village to city in search of job has changed the whole scenario. Within a family it is women, especially the home maker who are mainly victimized as they become more aloof than before. Hence, women often face the existential crises. To overcome depression and loneliness, women especially home maker tend to find a support outside their family circle.

---

[38] K. Jaishankar , Article on *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, 2011, CRC Press, Taylor and Francis Group. Pages 461. ISBN 978-1-43982-949-3// International Journal of Cyber Criminology Vol 6 Issue 2 July - December 2012

[39] *Ibid*

It is because of this reason that they tend to rely on strangers and make them their confident. With technology they easily get the chance to interact with them through chat rooms, video chat, instant message etc.

Predictable acumen guides as to consider that women are more emotionally expressive than men are. For this reason, it becomes easy for the culprit to win over the confidence of lonely women. In an emotional state, females tend to reveal a lot about their personal information. The miscreant can use this information against the women for causing harm and it is one of the prime reasons for causing some of heinous cybercrimes.[40]

- Partial Computer Illiteracy

  Partial computer illiteracy refers to the incomplete or fractional knowledge in landing or operating computer system and its application. A large segment of people are still aware of the safe and secured usage of computers. Initially very few people had learned computers by taking the help of the professionals. People started practicing computers with the help of their friends, peers, classmates etc. This resulted in the computer literacy but that was incomplete and therefore it had led to partial computer illiteracy. To large extend, studies revealed that computer literacy rate of males are higher than females.

  Common difference among men and women regarding the significance of internet related to four different issues. These issues are accessibility to internet, view point of both the genders about the technology, potentiality to use internet, different scope and ways of using internet. This also led to the victimization of women in this field.[41]

- Sociological Perspective: Nurturing Practices And The Patriarchal Indian Society

  Indian society is predominantly patriarchal in nature, and this is a major reason for women becoming victims of cybercrime. Females are taught to shun their voice for the fear of being stigmatized. Because of this type of nurturing practice, they become accustomed of ignoring imperative matters. Society decides the role of men and women. Men have to be serious, dignified, responsible, rational, unemotional, bold and dynamic whereas women

[40] *Ibid*
[41] *Supra* Note 1

must be joy, understanding, and patient, compassionate, emotional and must accept sacrifice for her family.[42]

It is the women vulnerability that gives the power to the miscreant for abusing her. Women, out of fear of being harassed by the police and losing support of the family, shun of the matters and this gives the culprit courage to repeat his wrong doing and the virtual world also gives the culprit courage to repeat his wrong doing and virtual world also gives him enough space to hide himself. The Center for Cyber Victim Counseling (CCUC) made a survey and found that only 35% of women have reported about their victimization, 46.7% has not reported and 18.3% has been unaware of the victimization. This proves that women prefer not to report about their victimization owing to social issue.

- Gap Between Legal Action And Technological Advancement

  One of the main reasons behind the increase of cybercrimes against women in India is the less legal protection. Law related to cybercrime are mainly associated with the augmentation of e-commerce and for this reason, the laws mainly covered commercial and financial crimes. It is the gap between existing legal protection and ever rising hike in the technological advancement that lead to widespread crime in cyber world.[43]

- Miscreant's Outlook : Cyber Addiction

  Internet is now easily available which has given the internet users both access and opportunity to misuse the resources. It is a virtual world where there is no physical existence of the person and anonymity facilitates open communication among the users that promotes development of online relationship. The undue use of internet means becoming addictive to it and such addiction also give way to victimization of female netizens.[44]

From the above, it could be deducted that women victims need faster restorative that women victims need faster restorative procedure to avoid further escalation of agony and trauma and they needs reluctant to approach the police for such restorative procedures. Thus the women victims of cybercrimes need different treatment from that of child victims or any financial fraud

---

[42] *Ibid*
[43] *Ibid*
[44] *Ibid*

victims. And in this research, I propose to establish that women from a separate group of cyber victims and deserve a different treatment in all sense.

SPECIFIC CRIMES TARGETTING WOMEN

"While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behaviour"

- Former U.S. Attorney General Janet Reno, Jan. 10, 2000.

Cyber world provides space for women. It gives her freedom to voice her opinion, pour out her frustration, anger; spell out her dreams. It is where she can share her world with others to find solidarity, affirmation & support. But danger lurks in the cyber world as in physical world in the form of stalking, vilification and verbal abuse. A woman is as vulnerable in cyber space as in physical space. Men intimidate her and seek to shut her up, discourage her from expressing herself. Increasingly, cyber space is being used to wreak vengeance, vendetta and to punish women.[45]

Cybercrime against women include harassment through email, cyber defamation, morphing, stalking, email spoofing, cyber pornography, cyber flirting & cyber bullying. Other crimes against women include posting vulgar comments & pictures on social media, morphed photographs, identity theft. Men are equally susceptible to all cybercrimes but women are in majority as victims. Studies shows that a majority of cybercrimes are related to obscenity and about 75% of victims are women. Youth and children are the next most targeted. For the purpose of this research, certain cybercrime specifically targeting women alone are highlighted.

(I) CYBER STALKING

Stalking refers to harassing and threatening behavior that an individual engages in repeatedly towards another person. Harassment by e- mails/Cyber teasing/Cyber bullying/Cyber flirting

[45] Dr. R Akhileswari- Article;- *Women Vulnerable to Violence in Cyber World too*. http//www.thehansindia.com/

is in effect can be considered equal to cyber stalking. In quasi legal terms, stalking can be defined as 'a willful course of conduct involving repeated or continuing harassment of another individual that actually causes the victim to feel terrorized, frightened, intimidated, threatened, harassed or molested and that could cause a reasonable person to feel so.[46] Cyber stalking is a recent phenomenon and women generally are the main target of this cybercrime. According to the Oxford Dictionary, Stalking means 'pursuing stealthily'. Cyber stalking involves following a person's movements across the internet by posting messages on the bulletin board or chat rooms frequented by the victim, constantly bombarding the victim with e-mails etc. Therefore cyber stalking involves threatening unwarranted behaviour or advances directed by one net user to another user using the medium of internet and other forms of online communication.[47]

Cyber stalking is an extension of physical form of stalking where the electronic medium such as the internet are used to pursue, harass or contact another in an unsolicited fashion. The term is used to refer to the use of internet, e-mail or other electronic communication devices to stalk another person. Stalking is a problem that many people especially women, are familiar within real life. Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & Internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc.

Cyber stalking can be categorised as follows

- On-line harassment and stalking that continues over the internet.
- On-line harassment and stalking that is carried out off-line.

Here under stalker attempts to trace the telephone number or residential address of the target. This crime is committed by collecting all the necessary personal information about the target such as his/her name, age, family background, residential address, telephone number, working place, daily retinue etc and put this information on social websites, porn sites pretending as if

---

[46] Nandan kamath, *Law relating to computers, internets and E-Commerce*, 4th edition,2009, universal law publications, p.248

[47] Definition by 'The National Center for Victims of Crime'

the victim is himself/herself posting this information and invite people to contact him/her. Generally stalkers use indecent language to lure people.[48]

As the internet becomes an even more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications, the net's intrusive capabilities as well as increased access to personal information. It is true that both men and women may be stalked but statistics show that the majority of victims are female. According to a survey on cyber stalking cases conducted for the period of 2000 – 2006 shows that in majority of cases the perpetrator is male and most preferred form of perpetration is through e-mail(38%) followed by message board(17%) and chatting(10%).[49]

Stalking under Information Technology Act, 2000

Previously, the only provision under IT Act that dealt with cyber stalking was S.66A[50] which was repealed by the Hon'ble SC as violative of freedom of speech and expression. In fact there were many cases that were initiated under S.66A of the IT Act, 2000. The Indian Information technology Act 2008(amended) also does not directly address stalking.

But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act 2008. Hence the most used provision for

[48] Dr. Shalini Kashmiria, Article;- *Mapping Cybercrimes Against Women in India*, International research journal of commerce and law (irjcl)volume -1, issue -5 (December 2014)

[49] Prof.R.K Chaubey, *An Introduction to Cybercrime and Cyber Law*, 2nd edition, 2012, Kamal Law House. P.399- 401

[50] Repealed **Section 66A of the Information Technology Act, 2000, which was inserted vide the Information Technology Amendment Act of December 2008, states:**

"Any person who sends, by means of a computer resource or a communication device:
(a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine."

regulating cyber stalking in India is section 72 of the Indian information technology act (Amended), 2008 which runs as follows;

Breach of confidentiality and privacy[51]:

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. And also sec. 72A of the Information Technology Act, 2000(amended in 2008), which runs as follows:

Punishment for Disclosure of information in breach of lawful contract[52]:

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.[53]

In practice, these provisions can be read with S. 441 of the Indian Penal Code, which deals with offences related to Criminal trespass and runs as follows: Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property , or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate , insult or annoy any such person, or with an intent to commit an offence, is said to commit criminal trespass.

[51] Section 72 of IT Act, 2000

[52] (Inserted vide ITAA-2008)

[53] *Ibid*

However, after the December, 2012 Delhi gang rape incidence, the Indian government had taken several initiatives to review the existing criminal laws. A special committee under Justice Verma was formed for this purpose and basing upon the report of the committee, several new laws were introduced. In this course, *anti-stalking law* was also introduced.

Whoever follows a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person or whoever monitors the use by a person of the internet, email or any other form of electronic communication or watches or spies a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person or interferes with the mental peace of such person, commits the offence of stalking. Provided that the course of conduct will not amount to stalking if the person who pursued it shows that it was pursued for the purpose of preventing or detecting crime and the person accused of stalking had been entrusted with the responsibility of prevention or detention of crime by the State , or that it was pursued under any enactment or rule of law, or to comply with any condition or requirement imposed by any person under any enactment, or, that in the particular circumstances, the pursuit of the course of conduct was reasonable.[54]

Whoever commits the offence described in S.354D (1) shall be punished with imprisonment of either description for a term which shall not be less than one year but shall extend to three years and shall also be liable to fine.

The gravity of cyber stalking came into focus in India when Delhi police was asked by ***Mrs. Ritu kohli*** to file complaint against an unknown stalker who flooded a series of e-mails to her. The person through the mail threatened her to either pose nude for him or give an amount of rupees one lakh. Initially she ignored the mail but got alarmed when she started receiving similar threatening letters through post. The accused threatened her that he would put up her morphed picture along with her phone number and home address. Adding to this, the accused did sent her the photograph which was confirmed to be the same photograph she had in her

[54] S.354D of the IPC

mail folder. She also received numerous unsolicited phone calls from strangers at odd hours for sexual favours.[55]

Based on her complaint, authorities traced his IP address and felt that the accused knew a lot about the victim and confirmed that he hacked kohli's email address & password through which he had an access to her photographs. The accused also chatted on behalf of the victim and distributed her phone number to various chatters. The accused ***Manish Kathuria*** was booked under S.509 IPC for outraging the modesty of a woman & he pleaded guilty. [56]

Reported Instances:

- In another instance, Chinmayee,[57] a noted singer from South India was harassed by perpetrators who posted threatening and obscene messages in Twitter and FB. The report said that Chinmayee made a formal complaint to the Chennai Police Commissioner on the ground that the perpetrators had threatened to "kill, rape and assault" her on Twitter and FB. Her mother was also targeted with vulgar expressions. The perpetrators did not stop with making obscene and vulgar comments towards Chinmayee; they also targeted her on the issues of supporting the cause of Tamils. The report stated that on the basis of her complaint, one of the accused was arrested under the provisions in the IT Act and the Tamil Nadu Prohibition of Women Harassment Act.[58]

- The cybercrime cell of Delhi received a complaint from a senior executive of an airlines company stating that he has been flooded with emails of morphed pictures of his wife showing her nude. These emails were also sent to all the colleagues of the complainant. The accused allegedly threatened to put up these mails on sex websites along with her phone number and address. Every time the accused sent a mail, he apparently created a new email

[55] Ritu Kohli v. Manish Kathuria//, P. Shah, Article on *Cyber Stalking & the Impact of its Legislative Provisions in India*, http://www.legalindia.in/cyberstalking-the-impact-of-its-legislative-provisions-in-india (last visited Nov. 4, 2012).

[56] (the case was registered before coming into force of I.T Act, 2000)

[57] Reported on the NDTV website on October 22, 2012

[58] Sam Daniel, *Chennai professor arrested for tweets about singer Chinmayi*, (October 22, 2012*)* Published @ http://www.ndtv.com/article/cities/chennai-professor-arrested-for-tweets-about-singer-chinmayi-283070 .

account. The police suspected the involvement of any disgruntled employee working in the office of the complainant. [59]

- ***Bhubaneswar Case***[60]- The Xavier Institute of management lodged a cybercrime complaint with the police in December 2004 that students & staffs of this institution are getting numerous obscene electronic mails. The students were also afraid of the online hacking, spamming & threatening. Police appointed technical experts to investigate & examine the matter. At first these were considered to be spam but later on students were over flooded with obscene mails & continuous sexual harassment through internet. At that time Bhubaneswar Police were weak to fight against cybercrimes as they were not trained enough to tackle the issue.
- A Delhi university law student has been accused of stalking & threatening a woman online over a year. He also created her fake profiles on social networking sites to defame her & made obscene phone calls. The victim while working in Delhi got acquainted with the accused and refused his marriage proposal. He assaulted her and she lodged a complaint on this behalf. After this he apologized and promised not to bother her in future. The accused also gave a written statement to police station that he will not stalk her. The victim later moved to Goa to live with her parents found out a fake profile of her & a photograph declared her to be his wife. The girl's marriage was called off due to this. A case under S.66 A of I.T Act was lodged.[61]

- ***Karan Girotra* v. *State***[62]

The only reported case till date to reach the judiciary on cyber-stalking is also merely an application to grant anticipatory bail. This case dealt with a woman, Shivani Saxena, whose marriage could not be consummated; as a result she filed for divorce by mutual consent. In the midst, she came across Karan Girotra while chatting on the internet, who told her he loved her and wanted to marry her. On the pretext of introducing her to his family, Girotra invited Saxena

[59] Dr. M Dasgupta, *'Cybercrime in India'*, first edition Reprint 2014, Eastern Law House, p.146- Reported by Time of India, 16th November, 2004
[60] *Ibid*

[61] *Supra* Note 5
[62] 2012 VAD (Delhi) 483

over to his house, drugged her and assaulted her sexually. He continued to assure her that he would marry her and began sending her obscene pictures from the night she was assaulted. He also threatened to circulate the pictures if she did not marry him. As a result, an engagement ceremony was performed between the two after which he continued to assault her and eventually called off her engagement to her. As a result, Saxena filed a complaint under Section 66-A of the IT Act.

Though the Court rejected the plea of anticipatory bail on the ground that nude and obscene pictures of Saxena were circulated by Girotra, an act which requires serious custodial interrogation, nonetheless it made some scathing remarks. According to the Court Saxena had failed to disclose her previous marriage to Girotra merely because she agreed to perform the engagement ceremony, even though such mention was made when Girotra had first professed his love to Saxena. The Court also took noted that there was a delay in lodging the FIR by Saxena. What is more shocking is that the Court held that Saxena had consented to the sexual intercourse and had decided to file the complaint only when Girotra refused to marry her.

This case highlights the attitude of the Indian judiciary towards cases involving cyber-stalking. It is appalling that factors as redundant as a delay in filing the FIR have a huge bearing on the outcome of the case. It is for this reason that more stringent legislations are the need of the hour.[63]

- In ***Raju Iyer* v. *Jawahar Lal Nehru University***[64], the respondent was found guilty of sexual harassment of the petitioner & have consequently imposed the penalty of compulsory retirement. He had sent 2 mails on 11.4.2008 and 12.4.2008 which carried vulgar and filthy contents & were graphic in nature which explicitly ask for oral sexual favours. He also made unnecessary phone calls at untimely hours to harass her in derogatory languages. The disciplinary committee of the university imposed the penalty of compulsory retirement against which the respondent filed appeal in High Court of Delhi. But the court upheld the disciplinary actions of the university and dismissed his petition.

[63] Dr.K.V.K Santhy, Professor, Nalsar University of Law, *An article on cybercrimes*, http://www.nalsarpro.org/
[64] WP(C) No.2541/2011

To be concluded, it can be stated that Out of the estimated 79 million population worldwide on the internet at any given time, we could find 63,000 internet stalkers traveling the information superhighway, stalking approximately 4,74,000 victims. As the Internet continues to grow, problems like cyber stalking will continue to grow. With the Internet being integrated into almost every part of human life, it is not a solution to simply suggest that turning off the computer will solve the problem. Internet users must learn to protect themselves from the dangers of Internet based crimes. It is becoming apparent that anyone, including man, woman, or child can become a victim. The effects of these forms of stalking upon an individual may include behavioural, psychological and social aspects. Specific risks to the victim include a loss of personal safety, the loss of a job, sleeplessness, and a change in work or social habits. These effects have the potential to produce a large drain on both criminal justice resources and the health care system, and it is therefore in the best interests of the authorities to take swift action when cases are presented to them.

CYBER PORNOGRAPHY

In the new millennium, world is running with globalization, liberalisation and communication convergence technology. With speedy development of science and information technology, the ugly face of crime chart is unfortunately rising higher to cause more and more human tragedy. Morality has sociological and psychological aspects. It is the individual's perception due to which human beings accept certain things as good and reject certain things as bad in society. It is dynamic with dynamic society and varies from person to person and society to society. There is no yardstick to determine what is moral and what is immoral.

We have freedom of speech and expression under Art.19 (1) (a) which is restricted by Art.19 (2) to maintain decency and morality. Due to the easy access to internet through new multimedia technology, cyber pornography and other cybercrimes are increasing every moment which poses a complex challenge for the legislation as it is easy to use, distribute or sell pornographic materials. There acts affects moral and psychological growth of society.[65]

The word pornography derived from the Greek word 'Porne' (prostitute) and Graphein (to write).It refers to any work of act or literature dealing with sex or sexual themes.[66] It is also

[65] *Supra* Note 15 at p. 134-135
[66] *Pornography*, MS Encarta Online Encyclopedia.

defined as sexually explicit material that sometimes equates sex with power and violence.[67] It is the sexual explicit depiction of persons, in words or images, created with the primary, proximate aim and reasonable hope of eliciting significant sexual arousal on the part of the consumer of such materials. Pornography is a verbal or visual representation of sexual acts. It is the portrayal of people as sexual objects for pleasure of others.

Pornography corrupts one's moral sense and instigates them to participate in various sexual offences. Pornography is nothing but marketing of women's sex.[68] It is an offence that affects women's life, dignity and reputation and can shake the moral conscience too. With the technological impact, women are depicted as an object which is longing to get involved into sexual acts.[69] Thus, all those respects once provided to them are no longer available in this technological era.

Legislative Approach

Freedom of speech and expression is recognized as Fundamental Right subjected to reasonable restriction to maintain law and order, public health, morality, decency etc under Indian Constitution. In ***L.I.C of India* v. *Prof. M.D Shah***[70] , Supreme Court of India held that freedom of speech and expression under Art. 19 (1) (a) is very basic and Fundamental Right of individuals which they acquire by virtue of birth as human beings. In a democratic country any attempt to gag this right except by reasonable restriction under Art 19 (2) is violation of Art.19 (1) (a) of the Indian Constitution and abuse of the basic democratic values. [71]

IPC: The law of obscenity which finds its place in S. 292-294 of Indian Penal Code is a British legacy. S. 292 are as follows:-

A book, pamphlet, paper, writing etc seemed to be obscene if it is;

- Lascivious ; or
- Appeals to the prurient interest, or

[67] Canadian Dictionary on English Language
[68] Definition of Encyclopedia of Ethics

[69] *Supra* Note 5 at p.425 – 426
[70] AIR 1993 SC 171
[71] Viswanathan, Suresh T: *The Indian Cyber Law*, New Delhi, Bharat Law House, 2001

- If it tends to deprave and corrupt person who are likely, having regard to all the relevant circumstances to read, see or hear it.

S. 499-502 prohibits defamation with punishment except exceptional cases. Sec. 505 prohibits making, publishing, distributing any statement or report with intention to conduce public mischief and prescribes punishments extend to 3 years or with fine or both.

S. 507 prohibits criminal intimidation by an anonymous communication and prescribes punishments extend to 2 years. S. 509 prohibits word, gesture or act intend to insult the modesty of a woman and prescribes punishment with imprisonment extend to one year or with fine.

Indian judiciary adopted 'Hicklin Test' to maintain decency and morality. In ***Ranjith.D.Udeshi* v. *State of Maharashtra***[72],the court held that indecent or immoral publication are prohibited by Art 19(2) of the Indian Constitution and S. 292, 293, 294 of IPC because their obscene publications corrupt the mind of younger generation. In ***Chandrakant Kalyandas Kakodkar* v. *State of Maharashtra,*** [73] the court held:-

"What is obscenity has not been defined under s. 292 IPC or in any of the statutes prohibiting and penalizing, mailing, importing, exporting, publishing and selling of obscene matters."

It is the duty of court to consider the obscene matter by taking an overall view of the entire work and to determine whether the obscene passages are so likely to deprave and corrupt whose minds are open to influences of this sort and into whose hands the book is likely to fall and in doing so, one must not overlook the influences of the book on the social morality of our contemporary society. In judging the question of obscenity, the judge in the first place should try to place himself in the position of the author and from the viewpoint of the author, the judge should try to understand what is it that the author seeks to convey and whether what the author conveys has any literacy and artistic values.[74]

[72] AIR 1965 SC 881
[73] AIR 1970 SC 1390
[74] *Ibid*

Then *Indecent Representation of Woman Act, 1986* related to pornography because it is an act to prohibit indecent reputation of women through advertisements or in publication, writing, painting and figure.[75]

- Obscenity under IT Act :-

The IT Act has covered all aspects of offences related to cyber pornography. It provides for the following

- Violation of the privacy (S. 66 E)
- Publishing or transmitting obscene material in electronic form (S. 67)
- Publishing of material containing sexually explicit act etc in electronic form (S.67 A)
- Child pornography (S. 67 B)

JUDICIAL RESPONSE

1. ***Raghuraj Singh* v. *Air Force Bal Bharti School (2001)***[76]

This case was filed in the Juvenile Court, Delhi on the charge of cyber pornography. The fact of the case is that the alleged accused was then a class 12th student who created a pornographic website as revenge of being teased by classmates and teachers. He listed in that website the names of his 12 schoolmate's girls and teachers in sexually explicit manner. He was then suspended by the school authorities. The juvenile court allowed his bail prayer. However, he was charged under S. 67 of I.T Act, S. 292-294 of IPC and Indecent Representation of Women Act. This is the most significant steps taken by law enforcement agencies in India.

2. ***Mumbai housewife harassed due to cyber pornography (2003)***[77]

In Mumbai, a housewife was receiving frequent filthy telephone calls, threatening her for sexual favour from one young boy in the city who got her phone number and name from an advertisement placed in a pornographic website in internet. Soon after the complaint filed by her husband, Mumbai police traced out that she was not the only woman who has harassed in

[75] Section 3 and 4 of the Act

[76] Available at http://presscouncil.nic.in/decisions/agiant_press/35.htm, (File No.CIC/LS/A/2011/000401)

[77] *Supra* Note 15 // The Hindu, Online Edition of India's National Newspaper; 27th Jan. 2003

this way and receiving such calls. Mumbai police traced that young boy who was accused and was arrested.

1.***State of Tamil Nadu* v. *Suhas Katti***[78]

This is the landmark case in the history of cybercrime in India which is considered to be 1st case where accused was convicted under S. 67 of 1.T Act, 2000 in India. In this case, the accused was known family member of the victim and was interested in marrying her. On her reluctance, the accused started harassing her through internet and posted obscene, defamatory and annoying message about her in the yahoo message group. The posting of message resulted in annoying phone calls to the lady in the belief that she was soliciting.

She filed a complaint in February 2004 and police traced the accused in Mumbai and arrested him. Subsequently, charge sheet was filed under S. 67 of 1T Act, S. 469 and 509 of IPC. The accused is found guilty under said sections and sentenced for rigorous imprisonment for 2 years and fine.

3. Delhi Public School and Multimedia Messages Service (MMS) Clip Case [79]

A Delhi public school boy allegedly filmed his girl friend in sexual act with him on his cell phone camera which is called as multimedia messaging service clip or MMS clip. This video was then forwarded by him to his friends and then his friends sent it to others. Gradually, it was available in almost all users and for small price with road side vendors. This clip was copied to VCD and offended for sale by a 23 year old IIT student named Ravi Raj. This clip was uploaded by him in a Mumbai based auction website Bazzee.com, which facilitated the online sale of property.

At first, accused Ravi Raj absconded and proceedings were initiated against Avinash Bajaj, CEO of Bazzee.com who was later on acquitted. Ravi Raj was arrested and then charged under S. 67 IT act, Section 201, 293, 294 of IPC. Ravi Raj was arrested on 14 December 2004 & Produced before Delhi court after 2 days and court remanded him. At first, bail was reserved and later on granted on 24th December 2004. The court directed him to furnish personal bond

[78]*State Of Tamil Nadu* V. *Suhas Katti* (2004)

[79] Supra Note 5 at p.461

of rs.50, 000 with two sureties, to surrender his passport and to co-operate for investigation as when required.

4. Gujarat University banned mobile the reason was that Gujarat local media published about an MMS porn clip of 10 seconds of a college girl was circulated in the campus and out.[80]

5. ***MMS clip case***[81]

The Chandigarh police registered an MMS video clip case between a woman and a city based professional slot on mobile phone camera. This case was registered u/d 292, 293, 499, 509 of IPC and S. 67 of IT Act for publishing, showing, circulating or distributing of obscene matter through electronic media may be computer, mobile phone and wireless.

6. ***Victims Of Spy Camera*** [82]

Accused and with the help of another person fitted a spy camera in the room of a lady teacher when she refused the friendship he offered. He was charged under S. 67 of IT Act for making CD's using computer, downloading her pornographic pictures. Then accused were released on bond.

7. Sayan Banerjee was arrested on the basis of complaint lodged by his wife that her husband were filming woman in nude by mobile camera and forced her to act for the racket.[83]

8. Pune police found out that landlord Mohan Kulkarni, fitted 3 web cams in one room occupied by girls. Police seized these and sent for decoding to the technology expert and sealed the bungalow. Investigation was on the basis of complaint made by 3 girls that landlord was refusing to return the deposited money and they suspected that they

[80] *Supra* Note 14
[81] *Ibid*
[82] *Ibid*

[83] *Ibid*

were filmed by that landlord. Thereafter, Kulkarni was arrested by police under S. 509 IPC, Art. 21 and 19(2) of Constitution and S. 67 of IT Act.[84]

9. MMS clip of school girl in Orkut, 2007[85]

In the year 2006 , a class 12th student was arrested by cybercrime cell of Noida police and he confessed that he along with his friends created the obscene picture of a girl circulated among friends and created a fake profile of that school girl in Orkut website. They were arrested under IPC, Indecent Representation of Women Act and S. 67 of IT Act, 2000. The victim girl was in clinical depression since she saw her profile in website which was posted by her school mates.

10. MMS Clip in Krishna Nagar, West Bengal Case

A former boyfriend aged about 22 of victim was alleged to have circulated nude pictures of a first-year College girl from his mobile phone after he got married with another girl. The girl and her sister had decided not to go to University even for examinations and not to face neighbours. The entire family was in ridiculous situation that they even could not step out of house due to taunts about those pictures. Father of alleged accused was an affluent bell metal trader. He was arrested on the as victim's father's complaint though alleged accused was roaming freely. The Officer-in-Charge of police station said that "during their affair, accused had taken video clips on his mobile phone which he circulated among youths in the locality. He also said that the boy's father knew and encouraged the same that was the cause of his arrest.[86]

11. State of Tamil Nadu v. *Dr. L. Prakash*[87]

This is a significant case where judiciary convicted accused under S. 67 of I T Act, 2000. The accused an orthopedic surgeon along with his 3 staffs were arrested by Chennai Police on December 2001. With the co-operation of one Ganesh, who assisted for making pornographic images of his clients forcefully & putting up those images of women patients on internet. He also circulated in abroad in CD's. Fast track court sentenced him with life imprisonment and

[84] *Ibid*
[85] *Ibid*

[86] Available at http://shodhganga.inflibnet.ac.in/23-01-2015

[87] W.P. M.P. No. 10120 of 2002

other 3 accused with 7 years rigorous imprisonment. Court also imposed fine of 1.27 lakh for posting prurient matter in electronic form under 1T Act, conspiracy and intimidation under IPC.

The concept of 'contemporary community test' was first acknowledged in Indian scenario in the Indian Supreme Court decision, *Ajay Goswami* v. *Union of India*. In this case the court held that the test of 'community mores and standards' is outdated in the context of the internet age which has broken down traditional barriers and made publications from across the globe available with a click of the mouse and hence in judging whether a particular work is obscene regard must be had to contemporary mores and standards.[88]

New multimedia technology is being misused and abused by criminals in cyber space.eg pornography, online child abuse, cyber spamming etc are increasing every moment. We have right to privacy that more confidential and private information due to be kept in secret and undisclosed because we wish not to disclose these to outsiders and the moment these are disclosed there will lose secrecy, confidentiality and privacy. Cyber pornography is not only national but also international legal challenge which needs intensive study, research and worldwide awareness.

CYBER DEFAMATION

"Who steals my purse steals trash…but he that filches from me my good name robs me of that which not enriches him and makes me poor indeed" [89]

The internet, as a global network of computers, has revolutionized the fundamental right to freedom of speech and expression. To author an article, book or poem and getting it published were the privilege of few in the pre-internet era. The multitude could never exercise their right to freedom of speech and expression in its true perspective in that era. The internet, on the other hand, is a global medium of expression. It provides limitless opportunities and ways of expression to its netizens, before a global audience. The fundamental right to freedom of speech

[88] (2007) 1 SCC 143// Vallishree Chandra & Gayathri Ramachandran, *The right to pornography in india: an analysis in light of individual liberty and public morality,* nujs law review 4 nujs l. rev. 323 (2011)

[89] Shakespeare in *Othello*

and expression has found a global medium that is truly democratic and luxuriously easy to use. Invisibility and anonymity are significant features of internet that lend fearlessness to speech and expression. As a medium of speech and expression, the internet is equally powerful for use as well as misuse. And online defamation is one such way of misuse of internet which in its form and extend capable of harming the reputation of an individual highly in the super highway of internet.

Defamation[90] is an intentional infringement of another person's right to his good name. It is the wrongful & intentional publication of words or behaviour concerning another person which has the effect of injuring that person's good name, status or reputation in society. A person's good name can be damaged if maligning statements are made out to someone other than that person i.e., the defamatory statement must be disclosed to a third party; there by satisfying the requirement of publication. When determining whether or not the defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation.[91]Even if there is no apparent damage to a person's reputation, the person who made the allegations can still be held responsible for defamation.[92]

In essence, the law on defamation attempts to create a workable balance between two equally important human rights. They are Right to unimpaired reputation and right to freedom of expression. In cyber society, both these ingredients are important. Protection of reputation is even more important in highly technological society, since one may not encounter an individual or organization other than through the medium of internet.[93]

In India, issue of defamation has so far been dealt under Indian Penal Code, 1860[94]. The Code makes no distinction between a slander and a libel. It defines "defamation" as: "Whoever by words, either spoken or intended to be read, or by signs or by visible representations, makes or

[90] According to *Black Law Dictionary*, defamation is the act of harming the reputation of another by making a false statement to a third person. Defamation in the Oxford Dictionary is defined as the offence of bringing a person into undeserved disrepute by making false statement.

[91] Supra Note 5 at P. 996-997

[92] Rodney D Ryder, *Defamation and the Net*, computers today, nov.2001.

[93] *Ibid*

[94] [Ss.499-502] of IPC

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 case hereinafter excepted, to defame that person."[95]

The main three ingredients of defamation are:

a. Making or publishing any imputation concerning any person

b. Such imputation must have been made by

(i) Words, either spoken or intended to be read; or

(ii) Signs; or

(iii)Visible representations

c. Such imputation must have been made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning whom it is made.[96] The Code also prescribes the punishment for defamation as: "Whoever defames another shall be punished with simple imprisonment for a term, which may extend to two years, or with fine, or with both".

In ***Amar singh* v. *Budalia K.S***[97] it was held that the criminal liability for defamation under IPC rests on the 'maker or speaker or author' and the 'publisher' of the defamatory content. The words 'maker or speaker or author' do not present any difficulty or doubt. The key word in the section is 'publishes'. In simple terms, the making known of the defamatory matter after it has been authored to some person other than the person of whom it is written, is publication in the legal sense.

In ***Bennett Coleman & Co.* v. *Union of India***,[98] the Supreme Court held that "publication means dissemination and circulation". That is, communicating defamatory statements only to the person defamed is not publication. The Code by highlighting that defamation could also happen by means of 'signs' or 'visible representations' has included every possible form of

[95] Definition as per s.499 IPC

[96] Ratan Lal & Dhiraj Lal, *Indian Penal Code*, 28th edition, Wadwa & Co. Publications, p.686

[97] (1965) 2 Cr.LJ 6593

[98] (1972) 2 SCC 788

defamation, including defamation in 'electronic form' as well. Instance of defamation in 'electronic form' includes generating, sending or receiving 'defamatory' e-mails, online bulletin boards messages, chat room messages, music downloads, audio files, screaming videos, digital photographs etc. on the Internet. Even sending 'defamatory' SMS, MMS, photographs and videos on mobile phones would be considered instances of defamation in electronic form. In other words, the Code is sufficient in itself to tackle any online defamation matter.

Provisions under I.T Act, 2000 - In India, a person can be liable for defamation both under civil and criminal law. With the new amendment in the Information Technology Act, 2000, India now has express provision on Cyber Defamation.

- Provisions under Information Technology Act, 2000

The repealed section 66A[99] was the sole section that dealt with any sort of offensive communication in the virtual world which criminalizes broadcasting of any information through a computer resource or a communication device, which was "grossly offensive" or "menacing" in character, or which, among other things, as much as caused "annoyance," "inconvenience," or "obstruction. And it was this provision that was capable of punishing the offender for online defamation too.

- Provision under IT Act, 2000 –

[99] Repealed **Section 66A of the Information Technology Act, 2000, which was inserted vide the Information Technology Amendment Act of December 2008, states:**
"Any person who sends, by means of a computer resource or a communication device:

(a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine."

ISPs[100] are not liable for any third party information, data, or communication link made available or hosted by them so long as- [101]

1. their function is limited to only providing access to communication system;

2. they do not-

(a) initiate transmission;

(b) select the receiver of the transmission, and

(c) select or modify the information contained in the transmission

3. they exercise due diligence in their duties and adhere to any guidelines which may be prescribed [102]

However, ISPs can be held liable in the following situations-

1. If they have conspired, abetted or induced in the unlawful act,

2. If, they fail to expeditiously remove or disable access to any information, data or communication link upon receiving the knowledge or on being notified by appropriate Government agency that such information, data or communication link is being used to commit unlawful act without interfering with the evidence.

Asia's first case of cyber defamation was filed in India in 2001. The case is ***SMC Pneumatics India Pvt. Ltd.* v. *Jogesh Kwatra***[103] where an employee of the plaintiff's company started sending defamatory emails to his employer and different subsidiaries of the company all over the world. Court in this case allowed an ex-parte interim injunction restraining the defendant from posting such remarks.

As per the *report published in The Telegraph*,[104] the perpetrator who was an ex-Indian army man had posted personal details of the victim and her husband in pornographic sites, including their residential addresses and had also created a fake profile of the victim in a wife swapping website. The victim's husband lodged an FIR when they started receiving unwanted phone

---

[100] Internet Service Provider

[101] As per Section 79 of the IT Act

[102] *Ibid*

[103] CS(OS) NO.1279/2001,Delhi High Court

[104] On 18th September, 2012[Vikash Sharma and Lelin Kumar Mallick, *Revenge whiff in e-crime - Man posts details of woman on porn websites*.(September 19,2012)

calls and came to know about the derogatory messages that were spread through fake email ids by the perpetrator. Even though the original complaint was with the Puri police, due to their incapacity to handle such cases, the case was later transferred to the Cuttack crime branch. The perpetrator was arrested under sections 66 C (which prescribes punishment for identity theft) and 67A (which prescribes punishment for publishing or transmitting material containing sexual explicit act in the electronic form) of the I.T. Act and Sections 292(which prescribes punishment for sale etc of obscene books,[105] 465(which prescribes punishment for forgery) and 469 of the Indian Penal Code (which prescribes punishment for forgery for ***purpose of harming the reputation***).

The one and the only cyber defamation case reported in India where a woman was victimised is ***State of T. N* v. *Suhas Katti***[106] where the accused who posted defamatory obscene annoying message about the divorced woman in Yahoo Message Group was held guilty by the court.

To conclude the existing law seems to be adequate to cope up with the problem of defamation against individuals and organization as a whole. But one of the important points to be noted is that the defamation against women needs special attention as they are the most affected groups in the field of cyber space. Unlike the traditional form of defamation, online defamation is different in nature, reach, extends & magnitude. They are in a way adds to the further vulnerability too.

The existing case laws in cyber defamation brought forth the fact that the women are less inclined to bring up a suit as to cyber defamation. The hike in cybercrime is directly proportional to the non-reporting of such cases. Compared to men, women are much hesitated to file a suit as it may further add to their disrepute by making it sensational. Effect of online defamation on woman is comparatively higher & such can destroy the marital relations of a woman. Not only that, it is capable of creating both psychological and sociological impact upon a woman. To this tragedy, the legislators were also silent spectators. Presently, defamation is

---

[105] Section 292 of the IPC in clause (1) defines obscene book, pamphlet etc as "a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the pruri-ent interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it".

[106] *Supra* Note 34

dealt under IPC. And the term 'cyber defamation' itself is unknown to I.T. Act, 2000. Therefore the need of hour is that the govt. should take a brave task of analyzing such crime, which are at the threshold & come up with recommendations in order to equip the existing legal machinery against such offence.

MORPHING

Morphing is editing the original picture by unauthorised users or fake identity. Fake users take help of social websites to download female's pictures and repost/ upload them on different websites by creating fake profiles after editing it. This amounts to violation of I.T Act, 2000 and attracts sec. 43 of the said Act. The violator can also be booked under IPC also. S. 43[107] of IT Act, 2000 deals with computer sabotage and provides that if any person without permission of owner/person in charge of computer does any of the following act such as unauthorized access to any computer, system, network, or data stored in computer, system or network, disrupts any computer, system or network, denial of any access to any person legally authorized to access, provides assistance to any person or facilitates access to any computer, system or network in contravention of provisions of Act/regulation/rules made there under, charges service availed by a person to the account of another person is liable to pay damages by way of compensation to the person so affected an amount which may extend rupees one crore. S. 66 C[108] deals with identity theft and provides that whosoever dishonestly or fraudulently making use of electronic signature, password or any other unique identification feature of any other person will be punishment with imprisonment up to 3 years and fine up rupees 1 lakh or both. S. 66D[109] deals cheating by personation and provides that whosoever does cheating by personation by means of any communication device or computer resource, shall be punishable with imprisonment up to 3 years and fine of Rs. 1 lakh or both.

REPORTED INSTANCES

- The recent ***Air Force Balbharati School case (Delhi)***[110] is a recent case comes under this category where a student of the School was teased by all his classmates for having a

[107] Section 43 of the *Information Technology Act*, 2000 as amended by Section 21 of the *Information Technology (Amendment) Act*, 2008.
[108] Section 66C inserted by the *Information Technology (Amendment) Act*, 2008
[109] Section 66D inserted by the *Information Technology (Amendment) Act*, 2008

[110] Abhimanyu Behera, Article on " *Cybercrimes and Law In India*," XXXI,IJCC 19 (2010)

pockmarked face. He, who is tired of the cruel jokes, decided to get back at his tormentors and scanned photograph of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. The father of one of the class girls featured on the website came to know about this and lodged a complaint with the police. Such acts can be penalised under I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC sec. 509 also.

- Two persons, including a juvenile were arrested for allegedly morphing the photo of a 12th pass-out girl and circulating the obscene MMS in mobile phones among his friends. The crime branch of New Delhi arrested a 24-year-old MBA employed with an automobile company for hacking into women's FB accounts and uploading her morphed nude photographs.[111]

- There are many other instances and one of which is that the Bandra unit of the Mumbai police crime branch arrested two men for allegedly using morphed photographs of women to blackmail them by threatening to upload the pictures on the Internet. The accused would morph photographs of the women to appear as nude pictures and mail them to the residences of the victims with a letter to extort money.[112]

- Police arrested a youth in Odisha who posted morphed vulgar & obscene photographs of a girl on social networking sites just because she had refused his marriage proposal. During the course of investigation, prima facie evidence was made against the accused & he was arrested. Investigation revealed that accused had become infatuated with the 22 year old girl & wanted to marry her. He even sent a marriage proposal to the girl's family through a relative. But after the girl rejected his offer- the accused, a school dropout but a computer savvy took it as a humiliation and posted her morphed vulgar photographs on social networking sites.[113]

---

[111] Paridhi Saxena & Anisha Malke, Article on *Cybercrime; another dimension of women victimization*, International Journal of Research & Analysis Volume 2 Issue 3, 2014// http://www.ijra.in/

[112] http://archive.indianexpress.com // 2-2-2015 (last seen)

[113] *Ibid*

- In another incident in Odisha, a 29 year old man has been arrested for allegedly posting several morphed obscene photographs and videos of a state minister & a girl in different websites based on a personal grudge against the girl's father whose astronomical predictions regarding the accuser's career went wrong. 13 years later, the accused that went unemployed, collected the photographs of the girl and morphed it with the education minister. When the photographs came to the notice of the minister, he lodged a complaint with the cybercrime police. When the accused was arrested he admitted the guilt, thus was booked under S.465 (forgery), S.469 (forgery for the purpose of harming the reputation), S.500 (defamation), S.294 (obscene acts and songs) IPC & S.67, S.67A of the I T Act.

This type of crimes is unknown to pre internet era. These are the adverse effect of advancement of technology even though it has been introduced as a boon to mankind. When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing. Victimisation of women through these modes of false representation can take place in two patterns as shown below:

(i) Representation made with the help of visual images of the victim: In this pattern, the targeted media could be FB and adult websites. Here the representation may contain images which portray the victim in indecent fashion. Such sorts of visual images can be accompanied by full personal details of the victim to enable viewers to know her more personally.

(ii) Representation made with false and offensive verbal description of the victim: In this pattern, the targeted media could be Twitter, FB groups etc. The representation may particularly target the victim's professional orientation, political ideology and may describe the victim in an offensive manner. The most identified motive or purpose for which these crimes are committed can be personal vengeance between the parties. [114]

VOYERISM

In an age of modern & revolutionized communication electronic equipments, the privacy of an individual is under siege. The video surveillance equipments has become smaller, more

[114] Debarati Halder , Article - '*Examining the scope of Indecent Representation of Women (Prevention) Act, 1986 in the light of cyber victimisation of women in India'* 2012

portable more easily concealed and more accessible to the general public; its clandestine application had contributed to today's cultural fascination with voyeurism. This advance video surveillance equipment has had a profound adverse impact upon our concept of privacy. India is not untouched by the adverse impact and the newspapers were flooded with various unsavory stories of surreptitiously concealed video cameras. There has been an unprecedented increase in incidents involving video tapping of private parts of unwilling females even in public places Lady's wash rooms or waiting rooms where one can reasonably expect his or her privacy.

A new form of video voyeurism also known as 'cyber peeping' has emerged in recent times where images of private area of subjects, mostly females are captured without her knowledge and then transmitted widely without her consent thus violating privacy rights. Video voyeurism is the act of secretly or discreetly photographing certain parts of the body mostly unclothed without the person's consent. It is in fact a very invasive and intimidating crime particularly in our society where the females are worshipped or respected. Many of the innocent victims, ladies or even minor girls have unwittingly becomes the object of video voyeurism websites whose privacy has been surreptitiously invaded using the high gadgets.[115]

With the development in video and image capturing technologies, observation of individuals engaged in private acts in both public and private places, through surreptitious means, has become both easier and more common. Cameras or viewing holes may be placed in changing rooms or public toilets, which are public spaces where individuals generally expect a reasonable degree of privacy, and where their body may be exposed. Voyeurism is an act which blatantly defies reasonable expectations of privacy that individuals have about their bodies, such as controlling its exposure to others.[116] Voyeurism is an offence to both the privacy as well as the dignity of a person, by infringing upon the right of individuals to control the exposure of their bodies without their consent or knowledge, either through unwarranted observation of the individual, or through distribution of images or videos against the wishes or without the knowledge of the victim.

---

[115] Neeraj Arora, Advocate, Article - *Prying Eyes on Privacy through Peeping Toms*, April 28, 2010, Archive for the Information Technology Act.

[116] Lance Rothenberg, Article on *Rethinking Privacy: Peeping Toms, Video Voyeurs, and the failure of criminal law to recognize a reasonable expectation of privacy in the public space,* American University Law Review, 49, 1127, (1999)

LAW TO DEAL WITH VOYERISTIC CONDUCTS

While in many other countries, there are now a variety of statutes dealing with voyeuristic conduct in place that seeks to protect these inviolable rights. India is not lagging behind to check this new form of felony due to the advancements in the technology. The legislature introduced section 66E via I.T (amendment) Act, 2008. This section recognize the right of privacy as inviolable and makes the felony punishable with imprisonment which may extend to 3 years or with fine not exceeding 2 lakh rupees or with both. This section recognizes the natural human desire of privacy.

With flagrant disregard, the video voyeur blatantly defies the legitimate desire for privacy by utilizing technology to observe, record and often to disseminate images of the very acts and the body parts that were never intended or reasonably assumed to be open to public inspection. In effect, the video voyeur disrobes the victim without knowledge or consent & in doing so, strips the victim of both privacy and dignity.

PUNISHMENT FOR VIOLATION OF PRIVACY[117]

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation - For the purposes of this section--

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

[117] Section 66E of I.T Act, 2000

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Punishment for publishing or transmitting obscene material in electronic form[118]. – whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt person who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on 1st conviction with imprisonment of either description for a term which may extend to 3yrs & with fine which may extends to 5 lakh rupees & in the event of 2nd conviction with imprisonment of either description for a term which may extends to 5 yrs & also with fine which may extend to 10 lakh rupees.

- Provision under IPC for Voyeurism

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 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

[118] S 67 of I.T Act

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.[119]

Explanation 1. — For the purpose of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

Explanation 2. — Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.

Voyeurism is a criminal offence in many jurisdictions across the world such as Australia[120], the United States,[121] Canada,[122] and the UK[123], which criminalises either the capturing of certain images, or observation of individuals, or both. However, the inclusion of voyeurism as an offence under IPC has closed several loopholes in the voyeurism law and is a precedent for the state to better work towards securing the bodily privacy of its citizens.

REPORTED INCIDENTS

- *Ghaziabad changing room incident* shines spotlight on video voyeurism where the store room owner was arrested for allegedly planting secret cameras to make clippings of the female customer while using the trial room, has shown adverse impact up on the concept of privacy. The peeping cameras are becoming technologically advanced, tiny and easily available at cheaper prices. They can be planted secretly with ease and its pervasive application has contributed to the growing fascination for younger generation obsession with voyeurism. These incidents are not unprecedented act and various newspapers have reported similar incident of

[119] S.354C of IPC
[120] Crimes Act, 1910
[121] Video Voyeurism Protection Act, 2004
[122] Section 162, Criminal Code of Canada
[123] Section 67, Sexual Offences Act, 2003

surreptitiously concealed peeping cams prying into locker rooms, changing rooms, swimming pools in prurient attempts to film unsuspecting victims. All these reporting are alarming being a very invasive and intimidating crime which also poses a fundamental challenge to individual privacy.[124]

- *In 2005*, accused S with the help of N fitted a spy camera in the room of a lady teacher who rejected the friendship request he offered. He was arrested and charged under s.66 of I. T Act.[125]
- Pune police arrested landlord Mohan Kulkarni, who fitted 3 webcams in the room occupied by girls. Police seized this and sent for decoding. Investigation was based on the complaint made by the girls that their landlord was not returning the deposited money & they suspected that they were filmed by the landlord. He was booked under s.509 IPC & s.67 of the IT Act.[126]
- Union HRD Minister Smriti Irani she spotted a hidden camera at an outlet of a Fabindia that was pointed towards the trial room she used while trying out some clothes after which Goa police registered a case of voyeurism. Four staff members of the Fabindia showroom near Panjim were detained as objectionable images were seen from the recordings of the hidden camera that was seized by police. Police have sealed the shop and inspected the showroom. The CCTV camera was installed on a wall, against a foot-high ventilation gap on the side of the trial room cubicle. A case has been filed under section 354 C (voyeurism) and 509 (intrusion into privacy) of Indian Penal Code against employees who were monitoring the cameras.[127]

Easy availability of these types of electronic gadgets at cheaper rate and caution less attitude of the society leads to such types of crime. Even though there exist ample provisions to deal with these issues, the ignorance and unawareness of the victims makes the problem extremely bigger. Hence it is considered as a social menace that needs to be curbed by the stringent application of law.

---

[124] Supra Note 14

[125] ibid

[126] Ibid

[127] http://www.firstpost.com// 8-2-2015

MOBILE PHONES AND CYBERCRIMES IN INDIA

Telecommunication was introduced in India long back in the year 1882. This was a mushroom growth of telecommunication after the advent of internet and mobile technology in India. It was on 15th august 1995, when the 1st mobile telephone service started on a non-commercial basis in India. On the same day internet was also introduced. After the liberalization and privatization in this area, India didn't look back. Telecommunication conquered the life of the citizens and in no time, India's telecommunication network became the 2nd largest in the world. In May 2012, there were 929.37 million mobile users in India.

IMPACT OF CELL PHONES ON HUMAN LIFE

Communication technology has left no aspect of human life untouched. Even our morning alarm clocks are replaced by mobile cell phones. Technology is constantly bringing advancements in our mobile cell phones. Internet enabled smart phones, tablets etc …are performing the functions of our computer, but one vital feature is missing and that is security. Rapid growth in the field of internet enabled cell phones to manage banking transaction, official and institutional transactions, rapid communications through emails, or social networks and many more. Virtually, one can perform the task of a computer in mobile; this means mobile phone is also vulnerable to the risk of fraud, theft of financial information and identity theft etc.[128]

CELL PHONES AND CRIME

When a thing is made or new invention is done or something has been explored which never earlier had been known to humans, the thing which is invented was surely with the intent to provide benefit to the mankind and for the growth and prosperity of world. But the history tell us that most of the time, when anything is invented, it was used for good cause and the bad cause i.e., for constructive as well as for destructive purpose. Internet which was developed to facilitate the communication across the world has been misused for harmful once like harassing, fraud, theft, hacking, pornography etc. recent reports have suggested that with the

[128] *Article on Mobile Phones And Cybercrimes In India*/http// www.lawyersclubindia.com//

advancement of the telecommunication technology, there is increase in cybercrime in the nation. The technological advancement has provided opportunities to the miscreant in the society, who is using cell phones for their selfish gains.[129]

IS CELL PHONE A COMPUTER?

The broader definition of cybercrime is; any crime where computer is used as either a tool or weapon. In common parlance, computer is understood to be a desktop or laptop. As per Information Technology Act 2000, computer means any electronic, magnetic, optical or any high-speed data processing device or system which performs logical, arithmetic or memory functions by manipulation of electronic, magnetic or optical impulses, and includes all input, output, processing, storage software or communication facilities which are connected or related to the computer in a computer system or computer network. This broad definition encompasses every gadget we are using in our daily life and mobile phones are just one of it.[130]

CELL PHONE CRIMES AND WOMEN

(A) SMS Spoofing is like email spoofing which looks to originate from an acquainted number but in reality it is spoofed and sends from some evil minded individuals. For example, if a woman receives her SMS in her phone in the middle of night from her spouse number asking her to bring cash as he met with an accident. The chances are that she would check his number and after confirmed it to be her husband's number, she would rush out with cash. This could be the response when a person is totally unaware of 'Mobile Spoofing'. Using a web based software; a cybercriminal could send anyone a message from any person's cell without even touching his cell.

(B) Disseminating mobile virus- viruses can not only affect computers but also mobile phone whereby its normal functions can be hampered. These viruses can spread through MMS, SD Cards, Bluetooth etc. In case of Commwarrior virus, it sends MMS to the contacts in the phone

[129] Supra Note 5 at P.569

[130] *Ibid*

and spread to other mobiles. The virus skull, replace the system application with non functional versions and the phone functionality will be disabled.

(C) Use of Mobile Phones for Extortion and Harassments – the real world offences are committed with the help of mobile phones as these criminals are attracted to latest technologies in order to escape from the clutches of law. One of the main factors is the anonymity in case of SIM card issued on false identification documents or address. In different incidents recently in most of the cases the criminals are using different SIM cards in different calls for ransom for avoid the possibility of being tracked by the investigation agency. Mobile phone can be used for furthering the crimes like stalking, harassment, threatening etc.

(D) Pornography on mobile phones – MMS is a service superior to the normal SMS where photographs, movies, videos, film along with the messages can be sent. This MMS service was used to interact more lively with friends, family and relatives but these services are highly utilized for sending pornographic videos from one mobile to other. Another mode is the companies which offer to download the pictures from the link of web addresses they used to send with the SMS's. The TRAI[131]that makes all the law related to mobile operators is silent when it comes to unsolicited messages from these service providers. Although TRAI has initiated action against unsolicited calls, termed as spam calls, the same spam messages do not fall under the ambit of these laws. The famous scam of Delhi Public School [132]Case involved the issue of MMS which was made and distributed by the accused to his friends via, MMS, which soon reached the market.

(E) Stalking – real world stalking can also be committed with the help of mobile phones. Just like emails, threatening messages can also be send through these networks. Through mobile phones constant phone calls, messages & MMS can be sent to intimidate or follow a victim. Just like computers, modern mobile phones serve an equal purpose in every manner thereby providing wide facility for a stalker to annoy, threat or harass a victim.

---

[131] Telephone Regulatory Authority of India// www.trai.gov.in//
[132] Available at http;//sify.com/news/ 16-2-2015

(F) Mobile Camera Misuse – highly influenced technological impact introduced cameras to mobile phone, which was once unavailable to normal people generally. By the advent of varieties of mobile phones in the industry, wide ranges of mobile phones were introduced in the market in lesser price. The easy accessibility of these products led to the misuse, of which women are more prone to moral hazards. In a recent incident in a hospital, the caesarean session of a lady was captured on mobile phones by the gynecologist and anesthetist and uploaded the video clipping on Whatsapp. These doctors were booked under I.T Act and IPC, & have already been suspended from service. Under the I.T Act, this is a serious offence. Two private T.V channels aired the video clip causing deep embarrassment to the woman and her family. The Payyannur police registered a case under s.354 of IPC & 66E (for violation of privacy), and 67(publishing obscene information) of the I.T Act.[133]

With the increasing use of mobile phones and the internet, women's privacy & dignity had been compromised. It is now easy to capture a woman's image using a mobile phone camera, morph it & then transmit to internet. The damage to dignity & pain such images causes are unimaginable. Like in the case of rape, violence against woman in cyber space leaves lifelong scars on the victim's mind. In the past few years, several suicides by women & more suicide attempts have been linked to cybercrimes.[134]

In ***Bennett Coleman & Co.*** **v.** ***Union of India***,[135] the Supreme Court held that "publication means dissemination and circulation". That is, communicating defamatory statements only to the person defamed is not publication. The Code by highlighting that defamation could also happen by means of 'signs' or 'visible representations' has included every possible form of defamation, including defamation in 'electronic form' as well. Instance of defamation in 'electronic form' includes generating, sending or receiving 'defamatory' e-mails, online bulletin boards messages, chat room messages, music downloads, audio files, screaming videos, digital photographs etc. on the Internet. Even sending 'defamatory' SMS, MMS, photographs and videos on mobile phones would be considered instances of defamation in electronic form.

---

[133] *Whatsapping of childbirth*- article was published on September 24, 2014

[134] Article on *Law to curb 'cyber assault' on women under consideration***,** http://www.thehindu.com/ July 6, 2009

[135] *Supra* Note 54

In the case of ***Ajit Singh @ Ajeet Singh* v. *The State of Jharkhand***,[136] the court denied the bail petition of the accused on the ground that he had circulated the pictures in which the victim was captured being raped through mobile phone. Along with sections 355(which prescribes punishment for assault or criminal force with intent to dishonour person, otherwise than on grave provocation) /376(prescribes punishment for rape) /387(prescribes punishment for putting person in fear of death or of grievous hurt in order commit extortion)/420(prescribes punishment for cheating and dishonestly inducing delivery of property) /499 (which defines defamation) /120B (which prescribes punishment for criminal conspiracy) of the Indian Penal Code, and Section 67 of I.T.Act (which prescribes punishment for publishing or transmitting obscene material in electronic form), the accused was also booked under Section 6 of the Indecent Representation Of Women (Prohibition) Act.

PROVISIONS UNDER I.T ACT, 2000

As per the term computer, as provided by sec. 2(i) of the I.T Act, mobile phones are encompassed n the definition of a Computer. Thus any information shared on the mobile phone though it may be talk, text or entry of information, they are encompassed in the purview of the I.T Act.

Section 66A which got repealed provided for punishments for sending offensive messages through communication services etc. This provision of law is parallel to provision to S. 294, 504, 506, 507 & 509 of IPC & only difference is that in this provisions of law the criminal uses his cell phone or computer to express his offensive feelings. The punishment prescribed in this section is imprisonment for a term which may extend to 3yrs and fine.

Newly added provisions in the I.T Act[137] provides for the punishments for publishing or transmitting of material containing sexually explicit act, etc., in electronic form. This is most important for teenagers. The trends of sharing pornographic material on cell phones are on

[136] B.A. No.239 of 2012 @http://www.indiankanoon.org/doc/57727136/. Accessed on 07.11.2012.

[137] S.67A IT Act, 2000

increase. The incident of indecent MMS is not unknown to anyone. This provision of law books those who publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct. This provision of law is analogous to S.292 & S.292-A of IPC. It provides for punishment on 1st conviction for imprisonment for a term extends to 5yrs and with fine which may extends to 10 lakh rupees. In the event of 2nd conviction, for imprisonment which may extends to 7yrs & also with fine which may extend to 10 lakh rupees.

I.T Act provides for punishment for publishing or transmitting obscene material in electronic form[138]. – whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt person who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on 1st conviction with imprisonment of either description for a term which may extend to 3yrs & with fine which may extends to 5 lakh rupees & in the event of 2nd conviction with imprisonment of either description for a term which may extends to 5 yrs & also with fine which may extend to 10 lakh rupees.

A mobile phone is just like a match stick. A match stick can ignite a lamp & can also ablaze a house. Choice is of the person having it. Alike is with mobile technology, one can use it to make life simpler or for satisfying any selfish gains by misusing it. A mobile phone also should be used with caution & Ignorance can also bring trouble. People must be sensitive towards suspicious or malicious information received on their mobile phones. They shall forthwith report against it. This will not only ensure their security but also security of others too. In this E-World, one must never forget the words of Fransis Bacon that knowledge is power, because in the world of computers; more you know about computers, the more you will know that you don't know.

In the end, it can be concluded that cybercrimes against women are basically the crimes directed against them with the motive of intentionally harming them and with the aid of modern telecommunication techniques like internet and mobile phones. Further though it is a global

---

[138] *Ibid*

crime, the whole population gets affected but the statistics say that the most vulnerable and prone section is the female section of the population. Reportedly a total of 103 cybercrimes including those of abusive e-mails were reported in 2013 as against 62 in 2012.[139] However, this is a rough estimate. The weakness in data collection may be because of fact that many crimes go unreported. Many women are either afraid or scared and many other use their own methods to tackle such situations. But this, in no way helps to reduce or even prevent the occurrence of cybercrimes.

Another reason for lack of proper statistics can be due to the fact that most of the existing laws and policies on information and technology do not mention anything regarding the cyber violence against women. When India started her journey in the field of Information Technology, the priority was given to the protection of e-commerce and communications under Information Technology Act, 2000 whereas matters concerning cyber socialization and communications were not included. India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes. This Act has widely covered commercial and economic crimes, which is clear from the preamble of the IT Act but it is observed that there is no specific provision to protect security of women and children, though there are few provisions to cover some of the crimes against women in cyber space under the Act[140].

Further development in technology, has aided the growth of cybercrimes despite of the fact of existence of law combating the cybercrimes. The number of internet users is growing and so cybercrime is bound to rise. This shows that our current nation-based legal methods have clearly not kept pace with this global threat of cybercrime against women. Hence, there is a shift from the use of technology for development and growth to crime and this calls for a shift to a more open and participatory form of law enforcement.[141] The need of the hour is to make

---

[139] Express News Service, Article on *Crime Against Women on the Rise in Hyderabad*, http://www.newindianexpress.com/cities/hyderabad/Crime Against Women on the Rise in Hyderabad (December 28, 2013)

[140] Shobhna Jeet, Article on *Cybercrimes against women in India: Information Technology Act, 2000*, Available at www.elixirpublishers.com (Elixir International Journal)

[141] Marc Goodman, Article on *How technology makes us vulnerable*, http://edition.cnn.com/opinion/goodman-ted-crime/ (July 29, 2012).

changes and amendments in the existing act so as to make it more appropriate and effective as a law for the women section of the society.

LEGISLATIVE APPROACH – US & UK

United States is one country which started the evolution of the internet & also the first to be affected & the first to retaliate to the ugly side of the internet, the cybercrimes. US saw a sea of growth in the cybercrime against women and created new laws to mitigate such crime and prevent future victimization. In this chapter, we discuss about various laws developed by US to prevent cyber victimization of women as well as conventional laws that were applied to prevent women in cyber space. The United States of America evidenced the rapid growth of the internet and the eruption of cybercrimes. Also in the US a surge in the cybercrimes against women was seen in the new millennium.

As per the WHOA[142] Statistics 0f 2000, among 353 respondents, 87% victims of cybercrimes were women & 68% of the harassers were men. As per this statistics, the victimization began mostly through e mails (39.5%), message boards (17.5%), & also chat rooms (15.5%), and other instant messaging or websites. The 2009-10 statistics of WHOA shows that women victims still remained a majority who forms the 73% of the victim ratio.[143] The policies and terms of the various US hosted internet service providers highlighted the fact that freedom of speech and expression, as has been guaranteed in the first amendment, is given high priority when regulating 'offending' content in the sites. Various literature reviews would show that the birth of various cybercrime regulating laws in the US, were marked by huge debates over probable clashes of constitutional rights and confusions. Laws were created one after another, publicly debated over their practicable usability and constitutionality; some stood the acid test of judicial accountability by the Supreme Court, some didn't. However, none was created with a sole purpose of safeguard women's interest over internet.

United Kingdom recognized the gender sensitive cybercrime as a potential danger to the society in the late 90's with wide spread discussion in the news media about stalking female celebrities through internet. In practice, cybercrime scenario in the UK is more oriented

[142] Working to Halt Online Abuse (WHOA)
[143] http://www.haltabuse.org/resources/stats/2010Statistics.pdf

towards analysis including drafting of legislations, for cybercrimes targeting national safety, financial security, corporate identities and information and child safety. Cybercrimes against women are comprehensively covered by the Protection of Harassment Act, 1997. By analyzing the statistical report of cybercrimes in UK, provided by 'Garlik', the online experts, for the year 2008-09, it can be seen that among 29.7 million adult internet users in UK, there are approximately 2,374,00 instances of online harassment.[144] By online harassment, the report indicates cases of mental distress of the victim, stalking, sending unwanted abusive mails containing hate messages, racial messages, threatening or blackmailing messages etc. It could be found that there is no separate good resource for cyber victimization of women in UK as well.

As indicated in the previous chapters there are various crimes associated with cyber space affecting whole mankind, and particularly women, like cyber stalking, cyber pornography, online defamation, cyber bullying, voyeurism etc. one of the common factor is its universality that all these crimes are committed worldwide, devoid of any barriers. [145]

CYBER STALKING IN USA

USA claims to have the most expansive regulation on cyber-stalking. This is because it has specific legislations dealing with the issue both at the level of the Centre and the states. At the Centre, the federal law dealing with the issue is *the Interstate Communications Act*.[146] This Act makes it a crime to transmit "any communication" in interstate commerce containing a threat that is intended to injure another person.[147] The phrase "any communication" is defined to include threats transmitted interstate through the medium of telephone, e-mails, beepers or the internet.[148] Once the crime is established, a sentence of five years punishment with a fine up to $250,000 is imposed on the guilty stalker. Despite its wide reach, this legislation is problematic because of the requirement that there must exist communication of a direct threat; therefore a threat which is implied does not become punishable under the Act.

---

[144] Report is available at http://www.garlik.com/cybercrime_report.php
[145] *Cyber space laws protecting women in UK//9-3-2015 (last seen)*
[146] 18 U.S.C. S.875(c) (2006)
[147] *Ibid*
[148] *Ibid*

This defect was highlighted in the case, ***United States* v. *Jake Baker***[149]where the case dealt with posting of sexually explicit material by Abraham Jacob, Alkhabas, student of University of Michigan under the pseudonym Jake Baker. Jake posted stories on an internet newsgroup describing the torture, rape and murder of a woman who had the same name as the Baker's classmate, at the University of Michigan. In addition emails were sent between Baker and a man named Arthur Gonda, from Ontario, Canada, who was a reader of his story. Over 40 emails were exchanged between the men discussing their desire to abduct and physically injure a woman of their area. A complaint was filed against Baker under Interstate Communication Act. Court held that the case did not satisfy the Credible Threat Standard as there was no specific class of targets to which the communication of two men are directed. And mere expression to indulge in perverse act was not sufficient to infer an intention to act in accordance with the desire. The class of women to which the mail was directed was too vague and not sufficiently specific to meet the standards required to invoke penalty under the legislation.

Therefore it cannot be seen from the case that such grave offences which involve the use of specific names also do not amount to cyber stalking under the current legal regime because they do not involve in the specific threat to the victim in question.

Another federal legislation that attempts to address the issue is the *Federal Telephone Harassment Statute*. Under this legislation it is a crime to use a "telecommunications device" to annoy, abuse, threaten or harass a person. In 2006, the definition of the term "telecommunications device" was amended to include *"any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the internet."* This legislation is hailed as landmark legislation, the fact that the requirement of direct communication between the stalker and his/her victim poses the same problem as the Interstate Communications Act.

The most effective federal legislation is the *Interstate Stalking Punishment and Prevention Act 1996*. This Act criminalizes conduct that results in a "reasonable fear" or "substantial emotional distress" in the victim as a result of the use of "any interactive computer service" by a person who "travels in interstate or foreign commerce. Therefore, by doing away with the "credible

[149] 104 F.3d 1492 (6th Cir. 1997).

threat" requirement, an essential of the Interstate Communications Act, the statute has made cyber-stalking more effectively punishable. The only weakness in the law is that situations where the stalker makes use of third persons to harass his/her victim remain unaddressed.

Moving now to the legislations in the states, Michigan was the first state to include online communications in its stalking laws in 1993.[150] According to the data provided by the National Conference of State Legislatures, as of 2012 all 50 states in the USA have laws that expressly address electronic forms of stalking.[151]

However, the legislations like the Michigan Code[152], also followed by California[153], Hawaii[154], New York[155], etc. only address "electronic communications" as part of their legislations that criminalize physical stalking. Again, by such amendment states have sought to penalize only that conduct which results in direct communications between the stalker and his/her victim, thereby letting stalkers who use innocent third parties to go scot-free. In addition, they follow the "credible threat", which makes cyber-stalking legislations ineffective. This is because an overt requirement of threat, an essential of the credible threat makes actions such as repeated sending of e-mails or requests on social networking websites non-criminal. For instance, a case in which vulgar, untrue letters were sent to the victim's husband was held to be outside the purview of the statute since no threat was exercised against the victim.[156] Moreover,

---

[150] Michigan Criminal Code, Stalking: S.28.643(8).

[151] *State Cyber stalking and Cyber harassment Laws*, National Conference of State Legislatures, March 23, 2012, http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx (last visited Nov. 2, 2012).

[152] Under the Michigan Criminal Code, "harassment" is defined as: "Conduct directed toward a victim that includes repeated or continuing unconsented contact, that would cause a reasonable individual to suffer emotional distress, and that actually causes the victim to suffer emotional distress. Unconsented contact under the Michigan Code specifically includes sending mail or electronic communications to that individual."

[153] California Penal Code, S.646.9(g),(h)

[154] Hawaii Rev. Statute, S.711-1106.5

[155] New York Penal Law, S.240.30

[156] Iowa v. Limbrecht, 600 N.W.2d 316, 319 (Iowa 1999).

communication must be directed towards the victim in order to satisfy the requirement of "credible threat".

Some other states such as Illinois[157], Mississippi`[158], Washington[159], etc. have specific legislations to address the menace of cyber-stalking. Much like the Interstate Stalking Punishment and Prevention Act, the only problem with these legislations is the requirement that the communication be addressed to a specific person; third-party stalking therefore continues to be an innocent activity. Only three states, i.e. Ohio[160], Rhode Island[161] and Washington[162] have sought to criminalize this form of cyber-stalking. These inconsistencies in the state specific statutes create a major problem in effective regulation of cyber-stalking, since the same conduct may be criminal in one state and innocent in the other.[163]

By the introduction of *'Violence against Women and Department of Justice Reauthorization Act, 2005'* cyber stalking were penalized and women were considered as the vulnerable victim. This statute amended the US Code so as to include cyber stalking as a penal offence. Thus cyber stalking is defined with three dimensional meaning which include;

(a) traveling by the accused from one place to another, in case of physical stalking; in case of cyber stalking, the word 'traveling' has been connoted by 'following the victim via emails or chat rooms or social networking sites etc';

(b) such traveling or cyber movement should be done with intend to cause physical harm or mental stress;

[157] 720 Illinois Comp. Statute, 5/12-7.5 (2002)

[158] Mississippi Code Ann., S.97-45-15 (2002)

[159] Washington Rev. Code, S.9.61.260

[160] Ohio Rev. Code Ann., S.2903.211(A)(2)

[161] Rhode Island General Laws, S.11- 52-4.2(a)

[162] Washington Rev. Code, S.9.61.260(1)(a)

[163] Louise Ellison and Yaman Akdeniz, Article on **'***Cyber-stalking: the Regulation of Harassment on the Internet'* [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, pp 29-48

(c) physical harm or feeling of physical insecurity or mental distress must be caused to the victim, or to her immediate family members or her spouse or her intimate partner.

In ***Gary Dellapenta* v. *California***[164], Dellapenta was charged for using the internet to solicit the rape of the woman who had rejected hid advances. He terrorized a North Hollywood woman by placing ads in her name which claimed that she had rape fantasies and provided her address. Many men who saw the ads came to her home and others disturbed her with obscene messages. At first the woman had no idea why men were banging on her door in the odd hours and when she learned about the ads she kept a note on her door explaining that the ads were false. In this case, the accused pleaded guilty to one count of stalking and 3 counts of solicitation of sexual assault and received a six year prison sentence.

The "free-speech" argument posed by anonymous cyber stalkers has been tried and rejected. Laws punishing cyber stalking crimes have been upheld in both state and federal Courts. In ***U.S.* v. *Bowke**r***, the facts revealed that Bowker began stalking a local news reporter, Tina Knight. He sent multiple emails saying such things as, "Thanks for my daily Tina Knight fix. Thanks for helping me get my nuts off," and "More Tina Knight, that is what I want and need." He also made remarks about watching her from outside her home. When she moved to another state, he continued emailing her and even sent a physical letter to her new address. When convicted of stalking and cyber stalking, he appealed on the basis that the statute was unconstitutionally overbroad. The Sixth Circuit found that the statute was constitutional on its face, and that it was extremely unlikely that any constitutionally protected speech would be affected. [165]

A ***male graduate from San Diego University*** stalked five female students on the internet for over a year. The female students were receiving hundreds of emails, as many as five a day. The

---

[164] Greg Miller, Man Pleads Guilty to Using Net to Solicit Rape, Los ANOIGLES TIfms, Apr. 29, 1999 at C5.// Joanna Lee Mishler, *Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if it Does? //* COMPUTER & HIGH TECHNOLOGY LAW JOURNAL// http://digitalcommons.law.scu.edu/

[165] 372 F.3d 365 (2004). // http://cyberstalking.web.unc.edu/caselaw/.

defendant pleaded guilty and faces up to six years in prison. He stated that the reason for the threatening emails was because he thought the women were making fun of him.[166]

In a ***2004 case, Robert James Murphy*** was charged with cyber stalking. He violated Title 47 of U.S Code 223 which prohibits the use of telecommunications to annoy, abuse or threat anyone. He was sending obscene messages and pictures to his ex-girlfriend for more than 4 years. The woman at first deleted the messages but later on collected it as evidences. Murphy pleaded guilty for two counts of cyber stalking.[167]

In another case ***New Jersey* v. *Dharun Ravi***[168], Rutgees university under graduate student was tried and convicted on fifteen counts of crimes involving invasion of privacy, bias intimidation, tampering with evidence, witness tampering and hindering apprehension or prosecution. On the first instance, Ravi and his friend Molly Wei used a webcam to view a private romantic encounter between Ravi's roommate Tyler Clementi and another man identified only as 'M.B'. In the second incident, Ravi urged the friends and twitter followers to watch via his webcam, a second tryst between Clementi & M.B. Though the viewing never occurred, Clementi committed suicide on Sep.22, 2010 and his death brought national & international attention. On May 21, 2012, Ravi was sentenced to 30 days in Jail, 3 years probation, 300 hours of community service and 10,000 pounds fine.

CYBER STALKING IN UK

The UK does not have a specific legislation to deal with cyber-stalking. There are three legislations that seek to criminalize such behaviour. The first of these legislations is the *Telecommunications Act, 1984*.[169] Under this Act, it is an offence to send a message that is "grossly offensive or of an indecent, obscene or menacing character" or a message with the purpose of "causing annoyance, inconvenience or needless anxiety" and knows that the

---

[166] Cyber Stalking, http://faculty.ist.psu.edu//

[167] First US cyber stalking case taking shape, Ken Fisher - Apr 25, 2004 //http://arstechnica.com//

[168] (N.J. Super. Ct. Crim. Div. 2012)

[169] Prof.R.K Chaubey, *An Introduction to Cybercrime and Cyber Law*, 2nd edition, 2012, kamal law house. P. 415

message is false, by means of a telecommunications system.[170] A telecommunications system under the Act is broadly defined to include communication through the internet. The glaring problem with the Act is that it does not criminalize conduct which uses a local area network to transmit data without relying on public telecommunications system.[171]

The second legislation on the point is the *Protection from Harassment Act, 1997*, which makes the offence of criminal harassment and the offence involving fear of violence subject to civil and criminal measures.[172] Under the Act, a person whose conduct "causes another to fear, on at least two occasions, that violence will be used against him" based on a reasonable man's assessment is liable to punishment for a maximum of five years and fine. It is sufficient that the accused ought to have known that his course of conduct would cause the other to so fear on each of those occasions. The Act also gives courts the power to impose restraining orders on convicted defendants; prohibiting them from further conduct which may be injurious to the victim.[173] Breach of such an order carries a potential sentence of five years imprisonment. Harassment includes alarm and distress.

The third legislation on the point is the *Malicious Communications Act, 1988*. By the Criminal Justice and Police Act, 2001, this legislation was amended to include electronic communications as well.[174] Under the Malicious Communications Act, a conduct using an electronic communication is offensive if it includes a message that is "indecent or grossly offensive" or a threat or false information that the sender knows or believes to be false. Therefore, it is evident that the standard relied on is that of a "credible threat" and the applicability of this standard may render any legislation intending to tackle cyber-stalking ineffective. As a result, activities such as poking or sending friend requests repeatedly may merely cause annoyance or distress to the person, but may not rise to the standard of being a credible threat or grossly offensive in order for it to be punishable under the Act.

---

[170] Telecommunications Act, 1984, S.43

[171] CP Walker, Article on *Criminal Libel* in P. Milmo and WVH Rogers, gatley on libel and slander 22.17 (1998)

[172] Protection from Harassment Act, 1997, S.2(2),4(4)

[173] Section 5 of PHA Act,1997-

[174] Malicious Communications Act, 1988, S.1; Criminal Justice and Police Act, 2001, S.43

The fourth in point of time is the *Communication Act, 2003* where s.127[175] speaks of improper use of public electronic communications network. It covers the sending of grossly offending and menacing messages via public electronic communication network. S. 127(1) (a) relates to a message etc that is grossly offensive or of an indecent, obscene or menacing character that are used for phone calls and emails. S. 127 (2) targets false message & persistent misuse intended to cause annoyance, inconvenience or needless anxiety. The judgment of ***DPP* v. *Collins***[176] UK High Court Decision sheds some light to what is 'menacing character' in which it observed that, ' A menacing message, fairly plainly, is a message which conveys a threat or which seeks to create a fear in or through the recipient that something unpleasant is going to happen. Here the intended or likely effect on the recipient must ordinarily be a central factor in deciding whether the charge is made out.

To determine whether a message is grossly offensive, one must apply the standard of open and multi racial society, the word must be judged by taking account of their context & all relevant circumstances. There can be no yard stick of gross offensiveness otherwise than by the application of reasonable enlightenment, but not perfectionist, contemporary standards to the particular message sent in that context. The test is whether the message is couched in terms liable to cause gross offence to those to whom it relates.

Finally, *the Protection of Freedom Act, 2012*[177] introduced two new offences of stalking[178]. S.2A creates the basic offence of stalking and consists of two elements -

---

[175] As per this section 127; (1) a person is guilty of an offence if; (a) sends by means of public electronic communication network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or (b) causes any such message or matter to be so sent (2) a person is guilty of an offence, if for the purpose of causing annoyance, inconvenience or needless anxiety to another, he- (a) sends by means of a public electronic communication network, a message that he knows to be false, (b) causes such a message to be sent; or (c) persistently makes use of a public electronic communications network.

(3) a person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

(4) sub section (1) & (2) do not apply to anything done in the course of providing a programme service (within the meaning of the broadcasting act 1990(c.42)).

[176] (2005) EWHC 1308

[177] http//www.wikipedia.com// 14-3-2015 (last seen)

[178] S.111 of Protection of Freedoms Act

(i) the person pursues a course of conduct; &

(ii) course of conduct amounts to stalking.

A course of conduct which amounts to stalking is defined as;

(i)Amounting to harassment; (ii) the acts or omissions involved are ones associated with stalking; & (iii) the person knows or ought to know that his course of conduct amounts to harassment of the other person. Stalking is deliberately left undefined and a non exhaustive example of conduct amounting to stalking is provided. The list includes- (i) following a person, (ii) contacting or attempting to contact a person, (iii) publishing any statement or material relating or purporting to relate a person/purporting to originate from them; (iv) monitoring a person's internet usage, email or other electronic communication; (v) loitering; (vi) interfering with property; (vii) watching or spying on a person. S.4A creates more serious offence of stalking involving a fear of violence or serious alarm or distress.

Tort Law and Stalking[179]

Tort law through its remedy of injunction could well be one of the remedies a victim of stalking may have against a stalker. For an injunction to be granted, it is enough to prove either damage or apprehended damage. The apprehended damage must involve imminent danger of a substantial kind or injury that will be irreparable. Tort law has been applied to stalking incident in UK. In ***Burnett* v. *George***, the plaintiff had been subjected to a series of assault, unwanted visit, damage to her house, telephone threats and telephone calls at unsocial hours. The Court of Appeal has granted injunction prohibiting the defendant from entering her property and assaulting, molesting and interfering with her by acts calculated to impair her health. In another landmark case of ***Burris* v. *Azadani,***[180] Court of Appeal recognized stalking as a civil tort, thereafter, allowed injunction to prevent it.

[179] Nandan Kamath, *Law relating to computers internet & e-commerce*, 4th edition, universal law publishing, p.253- 258

[180] [1995]1 WLR 1372

Criminal law & stalking[181]

It was in case of ***R* v. *Burstow & R v. Ireland***[182], that the House of Lords decided the stalkers who cause psychological injury to their victim can be prosecuted for the criminal offence of causing actual bodily harm or grievous bodily harm even when they have not physically attacked the victim.

REGULATIONS FOR ONLINE PORNOGRAPHY, OBSCENITY IN UNITED STATES

The *Encyclopedia of Ethics* has defined Pornography as the sexual explicit depiction of person, in words or images, created with primary proximity aim and reasonable hope of eliciting significant sexual arousal on the part of the consumer of such material. The *Canadian dictionary of English Language* defines pornography as, 'sexually explicit material that sometimes equates sex with power and violence'. To discuss cyber pornography in United States of America, one must refer to the 1st amendment of the Constitution for the protection of freedom of speech & expression in the US. But this right is not absolute and that is why defamatory statement, objectionable or obscene publications are not allowed. [183]

Regarding obscene publication one landmark case to be referred is ***Roth* v. *U.S***[184] the court held that obscenity falls outside the constitutional protection & should be judged by the average person applying the contemporary community standard & to the most vulnerable members of society.

In 1973 United States Supreme Court in ***Miller* v. *California***[185] brought forth three pronged test for determining whether work is obscene or not are as follows-

(i) Whether the average person, applying the contemporary community standards would find the work, taken as a whole, appeals to the prurient interest;

[181] Supra Note 38 at p.253- 258
[182] [1997] 3WLR534
[183] Supra Note 36
[184] 354 US 476(1957)

[185] 413US 15 (1973)

(ii) Whether the work depicts or describes, in offensive way, sexual conducts specifically defined by the State law;

(iii) Whether the work taken as a whole, lacks serious literary, artistic, political, or scientific value.

Using obscene languages and graphics in the electronic communications is considered as a crime under S. 2261A of Chapter 110A, Part 1 of Title 18 USC[186], which speaks about domestic violence, stalking and dating violence against women. Chapter 71, Part 1 of Title 18 of the US Code further denotes creation of obscene materials for distribution as a penal offence. However, obscenity in cyber communications with women and victimizing women by soft-core pornography in the cyber space still remains a debatable issue when seen from *Miller* vs. *California's* perspective. The First Amendment remains silent about 'consented pornography' with women models and regards viewing adult pornography as an extended right for freedom of speech and expression. This is apparent from the fact that the definition of "sexually explicit conduct" in S. 2256 of title 18 of the US Code, Part 1, Chapter 110 does not always include obscenity but complements more with soft-core pornography and further such conducts are considered as criminal conducts only when children are victimized by such acts. Further, pornography is not defined by any specific federal provisions.

Even though the term 'pornography' has been defined by academicians from the perspective of psychological and social behaviors, philosophical aspects etc none of those definitions could successfully impress the lawmakers. The reason for this could have emanated from the failed attempt of feminist activists to establish 'pornography' as an infringement of women's rights. Indeed, it is a hard truth that even though pornography fails to generate legal recognition in the US, often women of cyber age fall victims of court's blind support of the rights guaranteed under the First Amendment. [187]

However, the available legal provisions penalize unconsented filming of pornographic images of women and distribution of the same under Section 1801 of Chapter 88, Part 1 of Title 18, USC which discusses about video voyeurism and the distribution of the same. Even though the

[186] United States Code

[187] Halder, D., & Jaishankar K. ,*Cybercrime and the Victimization of Women: Laws, Rights, and Regulations.* (June, 2011) Hershey, PA, USA: IGI Global. ISBN: 978-1-60960-830-9 (E-Book)

US laws do not recognize definitions of 'pornography', such activities as described above, may be controlled by application of penal laws available in the Title 18 USC.[188]

As of now in America Cyber Pornography is regulated and for the same the traditional method mentioned in the Landmark Judgment of ***Miller* v. *State of California*** [189]is used along with other legislations. The legality of pornography is determined by the Miller test, the test dictates that the opinion of the local community on a specific pornographic piece is most important in determining its legality. Thus, if a local community determines a pornographic work to meet its standard for obscenity then it is more likely to be banned. This means that a pornographic magazine that might be legal in California could be illegal in Alabama. This standard on pornographic legality is extremely difficult to uphold for the internet given that the internet contains ubiquitous amounts of pornography.

The Court ruled that child pornography is not a form of expression protected under the constitution in ***New York* v. *Ferber***[190]. It has also upheld a state law prohibiting the possession and viewing of child porn in ***Osborne* v. *Ohio*** [191]

In ***Pope* v. *Illinois,*** it was held that the proper inquiry was not whether n ordinary member of a given society would find serious value in the allegedly obscene material but whether a reasonable person would find such value in it, taken as a whole. Thus the factors and standards for obscenity vary depending on the culture of the state.[192]

In ***US* v. *Zuccorini & US* v. *Brian Tod,***[193]Tod was arrested by FBI and Law Enforcing Agency, Canada for Online sexual exploitation of six year old girl. On this charge, U.S Court sentenced the accused to 30 months of imprisonment on charge of online child pornography.

LEGISLATIONS

[188] *Ibid*
[189] 413 U.S. 15 (1973)
[190] 458 U.S. 747 (1982)
[191] 495 U.S. 103 (1990)

[192] 481 US 497(1987)

[193] U.S Dept. of Justice, New York press release, 26th feb.,2004/www.cybercrime.gov.

The *Communication Decency Act, 1996* was passed to protect children against pornography. Under this Act, if any person knowingly transmits obscene material for sale or distribution in the state or foreign country by using computer service, it is prohibited as criminal offence. This Act imposes fine up to $ 1,00,000 & imprisonment up to 5 years for first time offence and for 10 years in subsequent offence.

Second attempt was made with the *Children's Internet Protection Act (CIPA) of 2000* which was intended to protect children from accessing to internet pornography. It requires filtering systems to all computers in public libraries as a condition for receiving federal subsidies for internet connectivity. [194]

Prosecutorial Remedies & Other Tools to end the Exploitation of Children Today Act, 2003 (PROTECT) US Supreme Court upheld the latest congressional effort to curb the spread of child pornography on the internet. The law makes it a crime to offer or solicit sexually explicit images of children.

CYBER PORNOGRAPHY/SEXUAL OFFENCES IN UK

Legal approach towards pornography, grooming adult females for pornographic purposes and 'forced pornography' needs renewed evaluation when it is seen from the perspective of digital age. Grooming for cyber pornographic purposes, defaming women by sexual way (by morphing her picture for defamation, putting her information in publicly accessible search engines etc) and infringement of cyber privacy of women etc, could be regulated by the Criminal Damage Act, 1977 (to cover physical damage to computer systems), Data Protection Act (for protecting personal information stored in the computer devices) the Computer Misuse Act, 1990 (related to the penetration, alteration and damage to computer systems), Protection from Harassment Act, 1997 and Malicious Communication Act 1998,Communications Act, 2003, (for the purpose of misusing public networking system and also for aiding or abetting for piercing cyber privacy in dishonest ways.[25] The Theft Act, 1968 (for fraudulently using victim's identity) and Equality Act, 2010 (to cover harassment of sexual nature or in other words, grooming for sexual purposes). Even though some of these Acts were drafted to safeguard e-commerce and related privacy issues, post 1999 laws are remarkably focused

[194] *Supra* Note 28 at P. 456

towards individual communications and related security issues. However, voyeurism and usage of the subject matter for adult pornography still poses serious threat to the question of online privacy for female victims. The only available legal answer could be Sexual Offences Act, 2003 which under section 67 criminalizes unconsented voyeurism and distribution of it.[195]

Some of the laws like Police and Justices Act, Sexual offences Act etc were targeted to control child pornography and not specifically to save women's interest. However, Section 63 of the Criminal Justice and Immigration Act, 2008 criminalize possession of extreme porn images in one's personal computer. The origin of the above provision could be traced to the heinous murder of a young female school teacher Jane Longhurst in 2003, which was suspected to be the result of one of the internet based atrocity, the violent pornography. The conviction of the accused Graham Coutt in 2004 made a huge impact in UK, demanding a ban of extreme internet sites promoting violence against women in the name of sexual gratification. This forced the government to pressurize shutting of the violent pornographic websites. But it was seemingly an impossible task for the government to ban such sites especially when many such sites originate outside UK where performers perhaps legally consented for the pornographic acts. Hence to eradicate the problem of 'importing' illegal sites, Criminal Justice and Immigration Act 2008 was drafted to ban possession of such sites using more strong language. It highlighted pornography and the possession of it, rather than obscenity and took a successful attempt to legally distinguish pornography and obscenity and victimization of women.[196]

In ***R* v. *Hicklin*[197]**, English standard of obscenity was propounded by Cockburn. The standard is whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences & in whose hand a publication of this sort may fall.

In ***R* v. *Fellow*[198]**, in this case an accused, 45 years old teacher was imprisoned for downloading and making child pornography from internet and for having pornographic video pictures of girls of his own school.

---

[195] *Supra* Note 46

[196] *Ibid*

[197] [1863] 3LR QB 360

[198] [1997] All ER 548

In ***William Mckirdy's Case***[199]**,** the accused 31 years old driver was held guilty for corrupting and depriving young girls of 9 to 14 years and for having sex with them. He recorded it and was imprisoned for 12 years.

LEGISLATIONS

(I) OBSCENE PUBLICATION ACT, 1959 & 1964

These two statutes constitute the major legislation to combat pornographic material of any kind in the UK. Section 1(1) of the 1959 Act provides the following test for obscenity:

For the purposes of this Act an article shall be deemed to be obscene if its effect or the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. Under Section 2(1), Obscene Publications Act, it is an offence to publish an obscene article or to have an obscene article for publication for gain. Under section 1(3) of the 1959 Act, publishing includes:

(a) Distributing, circulating, selling, letting on hire, giving or lending, offering for sale or for letting on hire.
(b) Where the article contains or embodies matter to be looked at or a record, showing, playing or projecting.

Section 1(2) of OPA 1964 makes it an offence to have an obscene article in ownership, possession or control with a view to publishing it for gain.

(II) TELECOMMUNICATION ACT, 1984

Section 43 of the 1984 Act makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character' and is an imprisonable offence with a maximum term of six months. In addition to dealing with indecent, obscene or offensive telephone calls, the Act also covers the transmission of obscene materials through the telephone systems by electronic means.

[199] November 1998 lawyer leeds.ac.uk.//www.cyber–rights/org/reports/child.htm.

(III) CRIMINAL JUSTICE ACT, 1988

Under sec. 160 of the 1988 Act as amended by sec. 84(4) of the CJPOA 1994, it is an offence for a person to have an indecent photograph or pseudo-photograph of a child in his possession. This offence is now a serious arrestable offence with a maximum imprisonment term not exceeding six months.

(IV) COMMUNICATION DECENCY ACT, 1996

The US Telecommunications Act 1996, including the provisions of the CDA 1996, attempted to restrict access by minors to 'patently offensive depictions of sexual or excretory activities', a provision clearly intended to cover the pornographic images and materials which are widely available on-line over the Internet.[200]

(V) CRIMINAL JUSTICE AND IMMIGRATION ACT, 2008

It is a piece of legislation in UK that criminalizes possession of extreme pornographic material. It refers pornography as, of such nature, that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal, which is grossly offensive, menacing or disgusting. The critical analysis of the above, may further open a question as where do women victims stand as per this law? Victims who have been "forced" to give consent to be portrayed in extreme porno images, or whose digital images have been doctored to make them / her appear as a "consenting" model may find it extremely difficult to prove their victimization especially when they are threatened by their perpetrators or when they are completely unaware of the fact that they had been portrayed in this fashion. Also, no law punishes adult models or photographer or the crew behind it as it satisfies the contract laws between the model and the agency who is filming the porno images. However, this specific provision remotely punishes distribution of such extreme pornographic videos in the internet as penalizing accessing and possessing such contents in personal computers may not be possible unless distribution of the same is also controlled.

[200] *Ibid*

CYBER DEFAMATION/BULLYING OR HATE SPEECH IN USA

Defamation is an act to portray somebody in a false light and deprive him of his reputation. Thus, defamation is a wrong done by a person to another's reputation. Oxford English dictionary defines it as "the offence of bringing a person into undeserved disrepute by making false statements (whether written or spoken)". According to the Black law dictionary, defamation is the act of harming the reputation of another by making a false statement to a third party. [201] The effects of online defamation could be exponentially worse than an offline incident due to the global nature of the internet and the fact that the statements can be accessed by virtually anyone. In addition to this, the issues of anonymity raises even more concern when dealing with defamation because the author or origin of the statement may be very difficult to trace depending up on the medium.[202]

Literatures show that cyber bullying; hate speech and consequently defamatory cyber speech against women are growing irrespective of existing preventive laws. Prevalent cyber cultures including ridiculing women with harsh taunting languages along with elasticity of First Amendment guarantees helped cultivating cyber bullying of women and cyber hate speech targeting women as a fast growing cyber offence against women. The hardest truth is, such cyber hate and defamations against women in the US are rampant not only for bloggers, but for women in the social networking sites, chat rooms and other cyber hangouts like YouTube, personal websites etc.

Often it is felt that the reason for the growth of cyber hate speech and bullying targeting women lies in the loose interpretations of First Amendment[203]. Truly, with the advent of time the expansion of the First Amendment rights has touched almost all the public communications devices like the motion pictures, radio and TV broadcastings, the print media and even the digital communication system including mobile phones, SMS and internet communications.

---

[201] Article by Vishal Vora, Article on *Defamation On Social Networking Websites*- http://www.mondaq.com/india//

[202] Article on Cyber and Online Defamation http//wikispace.psu.edu// 20-3-2015 (last seen)

[203] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". Amendment I, The Bill of Rights] provisions.

The advantage had been enormous, but the disadvantages even more gargantuan. In view of these judgments the courts in the 2007 case of ***United States* v. *Sutcliff***,[204] upheld a conviction of a defendant who posted threat messages in his website to kill a company's process server; uploaded the picture of the company's attorney and her daughter and published her home address. The message was accompanied by a voiceover clip played from a movie that featured the stalking of an attorney and his family. This particular case established online threats as unprotected true threats even though the defendant never sent his message directly to the recipient.

Apart from judicial interpretations of the limits of the rights guaranteed under the First Amendment; hate speech and bullying targeting women, defamation of women etc, are regulated largely by federal provisions which are meant to restraint workplace gender harassment and domestic violence or dating violence. In these provisions, harassment, stalking and sexual harassment eclipse the issues of victimization of women through online hate speech, flaming / bullying speech, defamatory gestures etc. This is evident from provisions such as Chapter 71, Part 1 of Title 18 of the US Code penalize using of obscene languages in communications through mail service and radio broadcasting. This has further been stretched to include prohibitory note for stalking violence which may include harassing the victim with obscene languages. Further, Chapter 119 of Part 1 of Title 18, US code criminalizes interception and discloser of wire, oral or electronic communications which to a long way prevents publishing of personal information and photographs for defamation purposes. But this does not provide a strong support for women who are attacked in the cyber space by anonymous perpetrators. [205]

It is understood that regulating non-sexual offensive speech against women which do not particularly generate threat, but which creates enough scope to demean women publicly, may not be possible in the US. Women's rights in the cyber space are often looked down upon when it challenges the rights guaranteed under the First Amendment by the typical 'internet

[204] 505, F.3d 944, 952-53 (9th Cir.2007)

[205] *Supra* Note 54

languages' which often include slang remarks about women. It remains much as a matter of ethics in the cyber space and not a subject to be regulated by laws.[206]

It often seems that present young generation of internet users, including teenagers and young adults have relaxed the water mark for slang languages targeting women to be "obscene" to a great extent. Absence of any direct gender sensitive prohibitory provisions in this respect often leaves the women victims to seek justice by applying provisions for Civil Rights under Chapter 13 of the Part 1 of title 18, USC along with other related provisions on defamation and harassing communications.[207]

Significant Cases

Arguably, the two most widely publicized cases dealing with online defamation have been ***Cohen* v. *Google*** and ***Doe* v. *Ciolli*.** In ***Matter of Cohen* v. *Google***,[208] Cohen, a fashion model, was suing Google and Google's subsidiary blog-hosting platform Blogger.com to unmask a user who had anonymously created a blog called "Skanks in NYC." The "Skanks in NYC" blog featured pictures of Cohen, captions, and text, which referred to Cohen as a "skank bitch" and accused her of being a "psychotic, lying, whoring . . . skank." Google did not have any substantive objections to the motion, but "refused to provide Petitioner with any information or documents with respect to the Blog unless it is required to do so pursuant to applicable law, regulation, legal process or enforceable governmental request." In reviewing the case for unmasking, the court determined that the use of the word "skank" was actionable, as skank refers to a person with poor hygiene, as well as the use of "ho" and "whoring," which refer to a person exchanging sex for money. The court decided that these phrases, in the context of the blog where they were used as captions to photos of Cohen, conveyed facts which were capable of being proven true or false. In this manner, the court applied a New York procedural test which reflects the common law summary judgment test described in Section IV of this report.

---

[206] *Miller v. California*, 413 U.S. 15 (1973), which established a three step test to prove obscenity as unprotected speech. http://www.law.cornell.edu/supct/html/historics/USSC_CR_0413_0015_ZS.html 24-3-2015 (last seen)

[207] Halder & Jaishankar, Article on *legal treatment of cybercrimes against women in uk*

[208] (N.Y. Sup. Ct. 2009)

As a result, the court ordered Google to provide the plaintiff with the identity of the anonymous blogger, and Google provided Cohen with the anonymous blogger's email address, among other identifying information. Cohen recognized the anonymous blogger as Rosemary Port, whom Cohen knew socially. After learning Port was the anonymous blogger, Cohen decided to drop her defamation lawsuit.

In ***Doe* v. *Ciolli*,**[209] Brittan Heller and Heidi Iravani, two law students from Yale, sued the online forum AutoAdmit, Anthony Ciolli, an AutoAdmit administrator, and several pseudonymous defendants under their AutoAdmit usernames, including "The Ayatollah of Rockn- Rollah," "pauliewalnuts," and "hitlerhitlerhitler." Heller and Iravani had each been the subject of numerous defamatory posts on the Auto Admit message boards. These posts included a variety of claims and statements about the plaintiffs, such as accusations that they had herpes or gonorrhea. After starting the lawsuit, the plaintiffs successfully won orders to unmask the defendants. However, several of the defendants could not be identified after the unmasking order was placed. For those defendants that were identified, the majority settled "somewhere in the low to mid four figures in exchange for promises from the plaintiffs not to publicize who they were."

Despite the common themes in state cyber harassment statutes, they vary substantially when it comes to the conduct in question. For example, Virginia limits its cyber-harassment law to the use of "obscene or lewd language" or the suggestion of "a lewd or lascivious act." In ***Barson* v. *Commonwealth***,[210] the Virginia Supreme Court reviewed a cyber harassment conviction of Barson for a series of emails he sent to his estranged wife and her friends and family. These emails contained statements calling his wife a "coke whore baby killing prostitute" and claiming that she has "risky gutter sex" and "sex with anonymous strangers" from Craigslist. On appeal, the Supreme Court determined that the emails, "as offensive, vulgar, and disgusting as their language may have been," did not meet the statutory definition of obscenity, which the court interpreted to follow the definition of obscenity from the ***Miller*** test, as the emails did not appeal to the prurient interest in sex. In contrast, an appeals court interpreted the word obscene, as used in the Illinois statute, under a broader dictionary definition to mean "disgusting to the

[209] 611 F. Supp. 2d 216 (D. Conn. 2009)

[210] 284 Va. 67 (2012)

senses" or "abhorrent to morality or virtue." As such, the full breadth of these cyber harassment laws may not be clear until they have been interpreted by their State's highest court.

In ***Polito* v. *AOL Time Warner, Inc.*,**[211] Polito was suing AOL[212] to unmask several users who were responsible for sending her "harassing… pornographic, embarrassing, insulting, annoying and… confidential" emails and instant messages from a frequently changing set of user names that she was unable to identify. Polito even changed her user name, but she continued to receive such communications afterwards. The court found that the conduct of the anonymous users was proscribed by the Pennsylvania cyber harassment statute, which covers communications including "lewd, lascivious, threatening or obscene words, language, drawings or caricatures" and repeated anonymous communications. The court thereafter ordered that AOL unmask the users.[213]

In 2006, a Broward County, Louisiana Circuit Court jury heard the case of a plaintiff named Sue Scheff who alleged the defendant had posted caustic messages against the Scheff and her company, claiming she was a "con artist" and "fraud". Jill Philipovic, a law student of New York University was attacked by anonymous perpetrators in the social networking site discussing her physical stature and the ways she could be raped.[214]

GENDER BASED OFFENSIVE COMMUNICATION IN UK

It is unfortunate that there are actually no separate gender protective laws to protect women from cyber offensive communication including sending defaming offensive messages or even obscene messages to female victim's inbox other than the following acts. Analyzing the *Communications Act, 2003*, it could be seen that this law was made to regulate cyber space (which was partially fulfilled by Protection from harassment Act, Malicious

[211] 78 Pa.D. & C.4th 328 (Lackawanna Ct. 2004)
[212] American On Line - AOL

[213] Alice E. Marwick and Ross Miller -Fordham University School of Law, Article on *Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape* [http://ir.lawnet.fordham.edu/clip] 6-10-2014
[214] Scheff v. Bock (US, 2006)// Paridhi Saxena & Anisha Malke, *Cybercrimes: Another Dimension Of Women Victimization*, International Journal Of Research And Analysis Volume 2 Issue 3, 2014// http://www.ijra.in/

communications Act and Telecommunications Act) and broadcasting in general. As such Chapter 1 of this Act under sec.127 penalizes improper use of public network communications with 6 months imprisonment or a fine not exceeding level 5 on the standard scale or both. It is to be noted that the term "improper use" has been meant to describe offensive communication including sending offensive / threatening / harassing mails / obscene remarks / materials etc which were also formerly penalized by *Malicious Communications Act.*

But the question is how far communication through internet can be offensive against women as per English laws? The legislations prohibit grossly offensive communication which also includes obscene remarks or materials. None as such covers gender-harassing remarks, gender discriminatory remarks or even gender based bullying remarks. This could be due to less legislative concentration on the gender sensitive issues other than basic equal payment or economic security guarantees. However, the new *Equality Act 2010* promises better management of gender based communication crimes in the cyber space from a holistic approach as this Act covers gender based harassments and victimization as prohibited conduct.

The law of defamation in the UK is governed by the *Defamation Act 1996* and the *Defamation Act 2013*. Both statutes however do not provide explicit definition of what is meant by defamatory. The Defamation Act 2013 (c 26) is an Act of the Parliament of the United Kingdom, which reformed English defamation law on issues of the right to freedom of expression and the protection of reputation. The Act changed existing criteria for a successful claim, by requiring claimants to show actual or probable serious harm (which, for for-profit bodies, is restricted to serious financial loss), before suing for defamation in England or Wales, setting limits on geographical relevance, removing the previous presumption in favour of a trial by jury, and curtailing sharply the scope for claims of continuing defamation (in which republication or continued visibility comprises ongoing renewed defamation). It also enhanced existing defences, by introducing a defence for website operators hosting user-generated content, and introducing new statutory defences of truth, honest opinion, and 'publication on a matter of public interest' or privileged publications (including peer reviewed scientific journals), to replace the common law defences of justification, and fair comment respectively. However, it did not quite codify defamation law into a single statute.

In the leading case of ***Sim* v. *Stretch***[215], Lord Atkin proposed that a defamatory statement is one which injures the reputation of another by exposing him to hatred, contempt or ridicule', or which tends to lower him in the estimation of right–thinking members of society'. It has been generally accepted since then that defamation refers to the publication of a statement which reflects on a person's reputation and tends to lower him in the estimation of right–thinking members of society generally or tends to make them shun or avoid him'.

Communications targeting specific individuals: If communication(s) sent via social media target a specific individual or individuals they will fall to be considered under this category if the communication sent fall within the scope of the Protection from Harassment Act 1997 and constitute harassment or stalking. Harassment can include repeated attempts to impose unwanted communications or contact upon an individual in a manner that could be expected to cause distress or fear in any reasonable person. It can include harassment by two or more defendants against an individual or harassment against more than one individual. [216]

Stalking is not defined in statute but a list of behaviours which might amount to stalking are contained in section 2A (3) of the Protection from Harassment Act 1997. This list includes contacting, or attempting to contact, a person by any means. When considering an offence under the Protection from Harassment Act 1997, the prosecution will need to prove that the defendant pursued a course of conduct which amounted to harassment or stalking. The Act states that a "course of conduct" must involve conduct on at least two occasions. Where it forms part of a course of conduct, "revenge pornography" - where sexually explicit media is publically shared online without the consent of the pictured individual, usually following the breakdown of an intimate relationship - may fall to be considered under this category of cases. Court orders can apply to those communicating via social media in the same way as they apply to others. Accordingly, any communication via social media that may breach a court order falls to be considered under the relevant legislation, including the Contempt of Court Act 1981 and section 5 of the Sexual Offences (Amendment) Act 1992, which makes it an offence to publish material which may lead to the identification of a victim of a sexual offence.[217]

---

[215] [1936] 2 All ER 1237 (HL)

[216] *Guidelines on prosecuting cases involving communications sent via social media*, http://www.cps.gov.uk/

A communication sent has to be more than simply offensive to be contrary to the criminal law. Just because the content expressed in the communication is in bad taste, controversial or unpopular, and may cause offence to individuals or a specific community, this is not in itself sufficient reason to engage the criminal law. As Lord Bingham made clear in ***DPP* v. *Collins***,[218] there can be no yardstick of gross offensiveness otherwise than by the application of reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context. The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates.

Issues of cyber privacy and related problems for women

The cyber space regulatory laws are partly gender sensitive in the US especially for cases covering stalking, domestic violence, dating violence and the extension of the same in the cyber space. While considering general privacy issues (excluding financial crimes), it is noted that women still remain vulnerable victims. Hacking and stalking are the most sorted crimes that invade the privacy of the victim. Video voyeurism and adult sexting are the two essential component parts of online privacy invading activities. While the earlier could be regulated by existing provisions, the later still needs proper legal attention. Along with these trends, privacy of women is constantly invaded through various social networking portals displaying personal information of women.

Even though online victimization of women done through privacy invasion is not directly regulated by any provincial or federal laws except for Violence Against Women and Department of Justice Reauthorization Act of 2005, several other federal legislations inspired by the rights guaranteed under the Fourth amendment (privacy in respect to search and seizures)[219] to a certain extent protect cyber privacy of women. Most notable of them are Section 2701 of Chapter 121, USC 18 (Part 1), which speaks about unauthorized access to data, Chapter 119 of Part 1 of Title 18, US code, which speaks about interception and discloser of electronic and oral communications etc; Section 1801 of Chapter 88, Part 1 of Title 18, USC, which speaks about video voyeurism, Section 2710 of Chapter 121, Part 1 of Title 18 USC

[217] *Ibid*

[218] [2006] UKHL 40

[219] Fourth Amendment guarantees right to privacy and the same right has been upheld by numerous judgments, such as Griswold v. Connecticut, 381, US 479, 484 (1965), *Olmstead* v. *United States* 277, US 438, 478 (1928)

which speaks about wrongful discloser of video tape rental or sale records etc. These laws definitely promise assurances for protection of private information of women stored in government records, hospital records as well as records of private organizations including workplaces, women networking sites etc. However, there is a strange correlation between First Amendment guarantees of free speech and the court's outlook towards exercising the same in the cyber space coupled with concerns regarding the individual's privacy. ***McIntyre* v. *Ohio Elections***[220] is one of the landmark judgments which followed this norm of upholding right to free speech and right to privacy. The court has recognized 'anonymity' and political views as an additional right in the cyber space. This goes a long way towards guaranteeing women internet users' right to privacy in the cyber space by remaining anonymous or hide under camouflaged identities, especially in cases of social networking sites and adult dating sites where risks of privacy penetration remains larger. But this judgment also opens gates for harassers to attack women under "anonymous cloaks". The 2004 verdict of ***Polito* v. *AOL Time Warner,***[221] however limited this extended right of the First Amendment by attaching tortuous and criminal liability for speeches and communications made under anonymous veil with intention to harass or defame others. It is hoped that this judgment will create awareness among the internet users in respecting the privacy and dignity of others, especially women.

In US it is unfortunate to note that in spite of precautionary rules and legislations, both the judiciary as well as ISPs advocate for the free speech having little or less concern towards privacy rights of victims. For instance, when a woman victim brings her painstaking case of public defamation, exposure and publication of personal information and subsequent harassments to the notice of these ISPs, either she receives a negative response which says the case does not violate the principles of the ISP and hence she is refused any help; or she gets a cold response with practically no 'trustworthy' promise. Perhaps the drafting language of the existing provisions need to be more broadly interpreted when the victimization involves cyber space, vulnerability and sexuality of women, the patterns of using the cyber space and the gravity of *mens rea*.

This chapter starts with statistics which show that women suffer more from cyber harassment related issues than men. Perhaps it is the vulnerability of women, the peculiar

---

[220] 115 S. Ct. 1511, 1516 (1995)

[221] *Supra* Note 70

feminine trends of using the internet and the laws drafted to cover limited liabilities and fast expanding meaning of First Amendment rights that make women victims more susceptible to be victimized in the internet.

With regard to the matter in UK, the presence of the actual rule through so many legislations could make it more confusing for the civilians as well as law enforcement officers of very small remote areas to understand the legal nature of the offence. It cannot be ruled out that due to lack of proper understanding, the victim might be rejected by the police itself from lodging a formal complaint. Could the Prevention of Harassment Act really save women from stalking and hate crimes? Could Equality Act really prove women's rights in the cyber space? Do these Acts guarantee that women will not be ridiculed for being "women" in the cyber space? Are these laws failing to prevent such crimes or rather encouraging these crimes due to back dated "phrases" or age old way of punishing the offender? Perhaps, Yes. Most of these laws have been drafted in the pre-internet era and they are being amended, modified, and refined to suit the needs of the cyber era.

Hence, a woman centric law is the need of the day in the UK and US which could cover all the cyber offences where women form majority part of the victims.[222]

CONCLUSIONS & SUGGESTIONS

The internet technology came into existence only in 1986, but it has shown unparalleled aggressive growth. It has exposed the society to a new world in which we can share our ideas and culture values and can enjoy all opportunities. But it is not a danger free zone. The internet technology came into existence only in 1986, but it has shown unparalleled aggressive growth. Cyber space has become an instrument for offenders to victimize or infringe women, the most vulnerable targets on internet. Internet has opened flood gates for various crimes against women in the cyber space. Even though, draftsmen and other world leaders who participate in EU conventions for establishing strict rules to control cybercrime against children, never considered victimization of women in the cyber space as a big issue like child pornography or

[222] Supra Note 54

hacking etc. which require an attention. Modern innovations have made life easier for women across the world, but side by side, these have also led to rise in the crimes of electronic violence against women.

The only legislation existing in India in cyber field is Information Technology Act, 2000. The object of the Act is crystal clear from its preamble which shows that it was created mainly for enhancing e-commerce hence it covers commercial or financial crimes i.e. hacking, fraud, and breach of confidentiality etc. But the drafters were unaware about the safety of net users. There is no doubt that cybercrimes are easy to commit with very little resources, but the damage can be huge to the security of women. Cyberspace is a new horizon controlled by machine for information and any criminal activity where computer or network is used as the source, tool or target is a global phenomenon.

Major Loop Holes of The Act:

A. Jurisdiction

The elementary problem which are associated with cybercrimes are jurisdiction. Cyber jurisdiction is the real world government's power and court's authority over internet users and their activities in cyber world. However, IT Act does not provide with solution for the issue of jurisdiction which is too important in legal perspective to decide the place of filing of the case.

B. Lack of Proper Definition and clarity

Secondly only broad kinds of cybercrimes and contraventions are covered under the Act. Initially only 10 offences were included under the Act and later on 13 new cyber offences were introduced by IT Amendment Act, 2008. But still there exist gap in law.

The term 'cybercrimes' or 'cyber offences' has not been defined under the Act which creates ambiguity as to what all acts can be inserted or committed so as form a cybercrime. Offences which are mentioned under Chapter 13 are exhaustive in nature. By considering the present scenario of the society, many offences still needs to find place under the IT Act as the developmental and innovative reach of the technology is unimaginably fast. Offences like cyber bullying, chat room abuses, watching pornographic websites etc are outside the purview

of IT Act even though some of these problems are attempted to be tackled with existing provisions and other laws.

Though the Information Technology Act talks about publishing of information which is obscene in nature, it does not specifically define what is obscene or what may be classified as Pornography. Even the punishment for pornography is not sufficient in India. Though legislations worldwide contain severe provisions for child pornography, there is no mention of the term 'child pornography' in India.

C. Role of Judiciary

Loss of evidence, lack of cyber army and lack of cyber savvy judges is another issue of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage which needs the appreciation is the Public Interest Litigation (PIL) which the Kerala High Court has accepted through E-mails. Today with the growing arms of cyber space, the territorial boundary seems to vanish. Thus, the concept of territorial jurisdiction envisaged under S. 16 of Code of Civil Procedure and S. 2 of Indian Penal Code will have to give away to alternative method of dispute resolution.

D. Exclusion of the term 'Mobile Phone'

The term Computer under IT Act is said to have included the 'Mobile Phones' but the Act as such does not make any provision specifically addressing mobile phones even though by interpreting certain sections inference can be drawn to offences related to Mobile Phones. The reason for such suggestion is the growing menace by the use of mobile phones in our society during the recent period which is comparatively higher. Initially mobile phones were considered to be a boon to the society in many ways but the same technological advancement hinders the privacy and dignity of individuals to that extend which creates moral, mental or psychological disturbances. Now it is high time to eradicate the issue as the victims themselves were unaware of the fact that they have been victimized. Because of the easy availability, cheap cost and additional applications installed within the system, much of the crimes are executed with it. Taking into account the present crime scenario, mobile phones plays a major role in any of the phase of the criminal activity. Thus, stringent regulations are the need of the day.

E. Lack of Self Sufficiency

IT Act cannot be called as a self sufficient Act because in the practical view point IT Act cannot stand alone so as to prosecute and punish a victim thereby curbing the issues in cyber field. It can be evident from the amendment provided to the Indian Penal Code, Indian Evidence Act. Still most of the cases are dealt with the assistance of IPC.

F. No parameter for implementation

This Act does not lay down the parameter for implementation. In India, government and police officials were not computer experts. Even Judges are not fully sensitized to technology. Role of judiciary is prominent while dealing with the conviction of offenders. Judges may not be an expert or efficient in pace with the current technological advancements. Lack of fine definitions and ambiguity in the provisions requires interpretations from the part of judiciary. Along with it, this Act does not mentioned as to how the extra territoriality will be enforced.

Cyber Regulation Appellate Tribunal (CRAT) is one man commission with law degree as an essential qualification. That will not serve the purpose. On contrary IT offences involves highly complex phenomenon which is beyond the understanding of common man and requires IT expertise in the field. Indian police is not well equipped to handle cybercrimes related investigations. Thus passing of IT Act can be seen as one of the means and not the end.

G. Penalty

IT Act 2000 provides for wide range of penalty for violations but by the introduction of IT (Amendment) Act, 2008 penalties got reduced which shows an unwanted leniency of the legislators towards the offenders.

Women Victims!!!

Violence against women is a violation of human rights and not a new phenomenon. It is always taking it shapes time to time in Indian history. With the passage of time, many feminists fought against women violence and for their empowerment in the society, but there is no end of her vulnerable life and her exploitation. Information technology brought a great revolution in the communication space for making world a 'Global Village' and giving equal realization of

rights to women. Invention of World Wide Web, mobile phones and tabs etc. changed women's standard of living. Although, these inventions came with huge benefits for us, but it too has some negative effects on our life and created great threat.

Women victimization is an age-old practice which still continues through today the forms of harassment have changed. The position of women has been vulnerable, always. Even if women are thought to be equal to men in various aspects, there still exists and erupts new ways of suppressing her. And in the present era of technology, women are not left out in the virtual world too. The use of cyber space and its attendant features of anonymity continue to influence negatively the social and cultural aspects of society. While the cyberspace has provided secure tools and spaces where women can enjoy their freedom of expression, information and privacy of communication, the same benefits of anonymity and privacy also extend to those who do criminal activities of violence against women. The use of internet to stalk, abuse, intimidate, harass, and humiliate women is palpable.

Even though ample provisions are provided under the Information Technology Act, all those need much clarity in the ever growing menace of cybercrimes. It does not mention any crimes specifically against Women. By considering almost all legislations in India, right from our Indian Constitution, it can be seen that Women centered provisions and special protections forms a part of it. Article 15(3) of Indian Constitution declares it to be Constitutional to make legislations favouring women. One of the reasons for such an inclusion is the high status once offered to 'Indian Women' which forms an integral part of Indian Culture. Reviewing the IT Act, other than the general consideration by the insertion of S.72, (privacy) no mention of any protection is sought to be achieved by the Act. By the introduction of such laws and punishments, which will be depicted as a warning, majority of the offences targeting women can be washed off.

On the Internet, women face large amounts of sex related harassment, abuse and discrimination on the basis of their gender, rather than their opinions, thoughts or beliefs. Bloggers, Tweeters, journalists and FB users with prominent profiles face rape threats, violent pornographic vitriol, sexual harassment, accusations of promiscuity, and various forms of humiliation on a daily basis – simply because they are women. This is a global problem with very little conversation or legal recourse surrounding it. For women who face such abuse, the first law to which they could logically recourse is Section 66A of the IT Act (repealed).

But unfortunately SC has struck down S.66A of IT Act in ***Shreya Singhal* v. *Union of India***[223]. Concerned by the recurring arrests made under Sec. 66A, petition was filed as PIL before the Supreme Court challenging the constitutionality of 66A. Thus, court declared Sec.66A as violative of Articles 14, 19 and 21 of the Constitution of India that guarantee citizens the Fundamental Rights to equality, free speech and life respectively and it could not be fitted into one of the exceptions listed in Article 19(2). The Court expressly recognizes vagueness and over-breadth as grounds for striking down S.66A. Vague and overbroad laws are problematic for a number of reasons. Vague formulations of domestic laws prevent individuals from knowing precisely what is prohibited and open the possibility of police misuse. As the Court observes, "It is quite clear that the expressions used in 66A are completely open-ended and undefined." It takes within its sweep, protected speech that is innocent in nature and is liable therefore to be used in such a way as to have a chilling effect on free speech. Sec. 66A was thus struck down because it damaged this fundamental aspect of democracy.

The deletion even though serves as a boon in one respect, has struck a major blow as far as female netizens are concerned. S.66A genuinely contained ambiguity in terminology and interpretation and because of this reason the same is prone to be misused. But what serves the purpose of the IT Act is to give protection against the cybercrimes only and the penal provision of the act was not intended to curtail speech and expression. And that is what should be highlighted in this respect when dealing with S.66A and it has nothing to do with citizen's freedom. The aim and object of the Act should have been given priority. Another point favouring S.66A is that it was the only provision under IT Act originated in order to give ample protection for female community as a whole. It was much wider in content that any form of harassment could have been inserted so as to punish a wrong doer. But ironically in the present scenario, this section could not find place at all.

Cases of cyber victimization of women especially through offences like the creation of fake profiles to describe the victim indecently, leaves a deep impact on the victim. Not only does this indecent representation remain 'alive' for a long time to create huge embarrassment for her, it also deters her professional as well as personal reputation. In most of the cases such

[223] 2013 12 SCC 73

profiles are left open for public viewing and are constantly updated in search engines. Impact of these virtual world offences has far reaching consequences up on a person. The IT Act, being the only law in cyber world turned out to be a half baked law. Even though India is one of the very few countries to enact IT Act to combat cybercrimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the security, integrity and dignity of women in general is not covered fully by this Act. Although acquaintance with technology is positive aspect that can be considered important for the development of any country but at the same time it is becoming the source to increase the crime rate with technology against the weaker section of the society.

The Information Technology Act, 2000 also applies to any offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves as computer, computer system or network located in India. However, in-case there is an offence committed by any foreign national under IT Act, 2000 legal assistance and cooperation will be required from concerned Authorities in the foreign country where the foreign national resides, for any investigation / prosecution/ extradition.

This is difficult as India is not a signatory to ***Convention on Cybercrimes*** which is the only convention emphasizing crimes in cyber space at international pursuit. The main objective of the Convention, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

The Convention aims principally at:

- Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime.
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form.
- Setting up a fast and effective regime of international cooperation.

As the speed of committing crime and impact thereof is greater in cybercrime cases and because electronic evidence can be easily tampered or is volatile, it is imperative to trace the offender in the shortest possible time and preserve original evidence. Moreover, tracing of offender in cybercrime cases may be more difficult due to availability of several techniques to camouflage one's identity. Effective investigation and prosecution of cybercrime matters requires quick action as evidence is volatile and failure to collect electronic evidence in a timely manner can defeat the whole process. It is only by an international co-operation and mutual assistance that this menace can be adequately punished as cybercrimes are multi-jurisdictional in nature.

In 2013, a comprehensive study was conducted by UN on the emerging problem of cybercrime with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. It was found that there is a large diversity of national cybercrime laws on international cooperation and there is need for harmonization of national legal frameworks-definition and scope of cybercrimes, investigative powers, and admissibility of electronic evidence. It was felt that the Convention and national legal frameworks need to be adapted by making suitable amendments to deal with rising cybercrimes.

It is imperative that India should sign any cybercrime convention that it will assist in many ways to increase co-operation and harmony between the member countries. They include-

- Types of criminal activity to be covered e.g. cheating by personating, forgery, misrepresentation, etc.
- types of judicial proceedings that stands covered
- Procedure for requesting assistance -- format, content requirements and authorities from and to which the request may be sent.
- cooperation in relation to seizure/production/confiscation/preservation of Documents
- process for Interception of electronic communications - preservation requirements
- cooperation in recording of evidence
- extradition procedure
- time lines for responding to requests for cooperation
- Standard for confidentiality and data protection.

Proposal of Cyber Rights for Women

1. Right to equality: Right to equality which suggests right against any discrimination of any sort, must be acknowledged as the primary right for women in the cyber space.
2. Right to live safely with dignity: this right may mean include the following:

(a) Right against 'forced pornography'

(b) Right against hateful communications including defamations.

(c) Right against hacking for the purpose of sexual as well as nonsexual crimes

(d) Right against stalking and following harassments

(e) Right against being abused in all the ways as discussed above in the internet.

(f) Right against blackmailing, threatening and cheating, and

(g) Right to live safely with dignity in the real space along with a clean virtual identity.

3. Right to communicate with others: This right may mean and include right to free speech and right to choose individuals with whom the woman feels comfortable to communicate. This may also include right to block or remove unwanted individuals who tries to communicate with her against her wish.

4. Right to make a livelihood from the cyber space and with the assistance of cyber space: This may include right to express her views and carry on her profession for a livelihood with the aid of cyber space. However this right also includes right to be protected from being used as a trade item for pornographic websites, obscene contents or even illegal women trafficking through internet without consent of the woman in concern.

5. Right to have "own space" in the internet: This right may include right to access and create a domain, right to create email ids, blogs and also access social networking sites and create profiles etc.

6. Right to assemble and association: This right may include right to create any web based association, women-only forums etc

7. Right to privacy: Right to privacy may mean and include right against invasions in her digital contents, private information and also private offline activities, which may be published online.

Proposal for Code of Conduct in the Cyber Space

Code of conduct for internet users: A set of code conducts for male and female internet users towards safeguarding women's interest in the cyber space are provided. These are as follows:

1) To respect other's right to privacy;
2) Restraining from indecent conducts in the cyber space;
3) Restraining from using cyber space as a verbal warfare and restraining from using abusive languages;
4) Restraining from using, modifying, republishing others contents without proper permission.

SUGGESTIONS AND STEPS TO TACKLE CYBERCRIMES

Besides, depending on legal system against cybercrimes, women have to be aware of cyber victimization by self, because time has come to reject the acceptance of silent. Moreover cyber laws are not universal, as they vary country to country. Today, every netizen wants to browse web privately and safely especially women. We should take some steps to tackle this problem. Here are some steps and suggestions that how women can save themselves of being victimized in cyber space and how they can make their online perceptions and experiences a safer one, are as follows;

(A) There is no mention of the word "women" in the Act: The amended version of the I.T. Act differentiates child pornography from adult obscenity and pornography but there is no mention of any provision in this Act to protect women exclusively. Since IPC has provision to penalize offences against "modesty of women" (Section 509 of the IPC), if similar ideologies were incorporated for IT Act, protection of women in the Indian cyber space would become more a swift job for the law and justice machinery. Societal trauma related to cybercrime against women wherein women as victim is considered more as an accused in her own case than victim must be removed.

(B) Change passwords time to time: In fact, people create easy-to-remember passwords because, it is simpler. If one wants to lower internet crime risk, changing password is a great way to make personal data and social networks safe and difficult to access for cyber criminal. Baffling or tricky password protect all accounts including cell phones, emails, landlines, banking, credit card etc. and are difficult for anyone to guess. Safest passwords contain letters, numbers and symbols. However, changing password can be very helpful to keep privacy safe.

(C) Avoid revealing personal details and address: This is the rule for women in particular who are business professionals and are very visible. They can use work address or a rent private mailbox. Thus, it can help them out in avoiding cyber stalkers. Moreover, women should avoid uploading more material on internet regarding their own information so that no one can easily access them. Avoid furnishing personal details such as family background, picture related to the people with whom you are socializing, your private moments etc on social websites like Face book, Google+, Twitter, LinkedIn as it can be easily misused.

(D) Beware of unsolicited calls and messages: Woman should avoid unwanted or unsolicited phone calls and messages because cell phone may be monitored. If it happens again and again, one should try to record phone calls of harasser and report to the police. Besides, they should discuss and share the problem regarding cyber harassing with their trusted ones like parents, mates or spouses etc.

(E) Understand privacy settings of social network: Social networks and other online content and service providers all have privacy policies and private settings. One must try to understand privacy policies and adopt privacy settings that help in protecting oneself from any potential risk or online harm. So, we must have the knowledge about privacy settings of social networking.

(F) There must be clear cut and uniform guidelines for the ISP fixing liability and accountability. The increasing number of crimes against women is a huge concern for any state however, cybercrimes make it even more challenging as criminals have the

opportunity to create fake identities and then after indulge in illegal activities. To counter this government should make stricter laws to apply on the Internet Service Providers (ISP), as they alone have the complete record of all the data being accessed by anyone surfing on net. ISPs should be made to report any suspicious activities that any individual is indulging into, this will help to curb crimes in nascent stage.

(G) Need to have strong and practicable security policy handling mobile technology and wireless technology along with computer technology and multimedia technology. Police authorities investigating the cases related to cybercrimes must not only be given IT Training but also be trained in dealing women victims psychologically. Thus there is dire necessity of psychological up gradation of women victims which require sensitization of police authorities.

(H) Need of specialized cybercrimes court with expertise, in the field of information Technology We need training of law enforcing agencies and IT professionals to curb the menace.

(I) Rigid and stringent laws: India must bring in more rigid and stringent laws for cybercrimes against women in the cyber space. It is evident that present India's Information Technology Act includes only few sections for cybercrime, especially against women, hence to curb cybercrimes, either IT Act must be re-modified or a separate law on cybercrimes should be created. Proper law and order against crimes may lead to create good society.

(J) Maximum punishments under the Act are bailable thus there is a necessity to increase punishment so as to have deterrent effect.

(K) Seminars and workshops for better understanding of cyber victimization: Police, Lawyers, social workers, and NGOs must be invited to education institutes, clubs, corporate offices, awareness-campaigns, seminars and workshops to discuss about legalities and illegalities of cyber conduct among adults inclusive of both genders. Reporting of cyber victimization at all levels directly to the police and NGOs working cybercrimes must be encouraged. Secondly, workshops and seminars must be conducted for the police personnel

for better understanding of such kinds of victimization and quick responses towards the complaints.

(L) Awareness campaign against cybercrimes: Awareness campaign must be set up from the grass root level such as schools, collages etc about cybercrimes like stalking cheatings, economic cheatings, defamatory activities, misusing emails and social networking websites, virtual rapes, cyber pornography, email spoofing etc. These campaigns can be fruitful in paralyzing cybercrimes.

(M) Need to adopt Uniform Law worldwide because Cybercrime is not only a national problem but also an international problem. There is need to adopt specific laws on jurisdiction and international co-operation following European Convention on Cybercrime, 2001.

CONCLUSION

Indian current scenario exemplifies many instances of female abuse and exploitation in the technological era which can be brought forth with a recent instance of Smrithi Irani, Union Minister, HRD who spotted a camera in the changing room of Fabindia, a boutique. This very issue turns on many questions with regard to the safety, security, dignity of Indian women and the culture claimed to be owned by our country. One of the glaring questions in this regard is that, 'So where can a woman be safe?'

It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes. This Act is widely covered commercial and economic crimes which are clear from the preamble of the IT Act but it is observed that there is no specific provision to protect security of women. By taking into account the positions of US and UK, there exists much legislation to deal with the issues. In spite of certain enactments got introduced in the pre internet era, much of the legislations in US and UK got birth and capable to curb the issue, either by amendment or got enacted after 2000. However in India, there are few provisions to cover some of the crimes against women in cyber space under IT Act. Still IT Act depends upon Indian Penal Code to deal with the crimes in virtual world.

Crime should be dealt with in their nascent stage and cut off at the first instance so that they don't develop into something serious. It would be best to amend the Indecent Representation of Women (Prevention) Act, 1986 to include within its scope all these different cases since it was made specifically with an object to 'aid in addressing the problem of increased objectification of women and thereby ensuring dignity of woman.' Therefore while the IT Act, 2000 is gender neutral, this act can specifically target and eradicate notion of cybercrime against women at very first stage. Another benefit is that this act, if amended can punish 'all forms of indecent representations' and it will thereby be wider in its ambit and scope. Anything that might not be lascivious or cater the prurient interest but still is considered as indecent would also be punishable. Any depiction in any manner in the figure of the woman, her form or body or any part thereof in such a way as to have the effect of being indecent, derogatory, or likely to deprave, corrupt or injure public morality, 'is still indecent' and such that shall be included in the purview of this act.

Another important aspect is that, only with the help of international treaties and conventions along with the co-operation of other countries that most of the problem pertaining in the field can be washed off. As cybercrimes are trans-boundary in nature co-operation with other country with regard to extradition and prosecution becomes a must. Speedy disposal of the case is relevant as the evidences are intangible in nature and it shall only be possible if and only if all the states stand together to drive away the issue. In this direction the European Union has taken certain initiative in the form of *European Convention on Cybercrimes, 2001* supported by many other international organizations such as the World Intellectual Property Organization (WIPO), the Copy Right Treaty, 1996, to which many countries like United States of America, European Union and Canada are signatory.

Thus, India also needs certain major changes like *United States Internet Crime Complaints Centre (IC3)* and *Cyber Police in China* for reporting and tracing out domestic crimes on Internet. It is for the people to understand that violence against women is nothing but a manifestation of gender discrimination and inequality in gender power relations. The only international convention pertaining to virtual world being "*Convention on Cybercrimes*" to which India should be a signatory, also helps to achieve a uniform standard to deal with the issue at global level. Women should understand that the time has come to reject the silence or

reticence and come forward for fighting against cybercrimes and for their rights. And most importantly each individual should be aware of their own rights and duties that he owes to other members of the society. Swami Vivekananda had said,

"The nation which doesn't respect women will never become great now and nor will ever in future" and in order to make India a great nation, let us work towards giving women their much-deserved status and place".