Legal Treatment of Cyber Crime against Women- Global and National Perspective

Sarmistha Neog*

Abstract

With constant evolution of human society the social structure also took its pace. It results in transformation of societies from enlightenment led by reason to modern industrial age led by technology with reason and finally landing into an information society led by electronically processed information via networks. With information, communication develops, leading to interpersonal relationships- relationship not based on attraction and direct interaction but via social networking sites. Slowly it becomes an object of fantasy. Activities which were earlier committed in physical space are replaced in cyber space due to the ease of anonymity. It results in growth of new forms of crimes like- cyber defamation, cyber stalking etc. the vulnerable groups like women, children mostly of adolescent age suffers from cyber victimizations. In this paper, the author has made an effort to examine the various issues related to victimization of women in cyberspace and tried to map out the impact of this virtual world in their physical life leading to trauma, fear, depression, harassment, defamation etc. In this respect, the author has tried to analyze and evaluate various cyber related laws in global as well as national forum to analyze how much they are potent to protect women in cyberspace. Despite having various laws, women are still being harassed and victimized in cyberspace. Therefore, the author firmly believes that there should be uniformity in cyber related laws for fencing this borderless crime in all the counties. Besides law and legal institutions, the solution to the problem of abuse and harassment need to be searched in the societal norms and values.

Keywords: *Cyberspace, Cybercrime, Victimization of Women, Cyber-laws.*

Introduction

We live in a world which is technology driven and is unique in the sense that it creates a beautiful interface between hardware and software[1]. This interface again creates a world out of science fiction, having no geographical boundaries. Thus, today's information societies are underpinned by digital technology creating a dynamic virtual space by the networks of 'machine clones' i.e., computers.

This dynamic virtual space has been termed as cyberspace. Therefore, while Internet is a fact, cyberspace is a fiction. It is an intangible space created by the medium of Internet. It has no physical attributes yet one can see it, hear it and interact with it.[2]

Thus, cyber space is dynamic, undefined and exponential. However, cyberspace does not exist in isolation but is intricately connected to the physical world. As a

*Assistant Professor, University School of Law and Research,USTM

[1] The New Oxford Dictionary of English defines Internet as an international network providing electronic mail and information from computers in educational institutions, government agencies, and industry, accessible to the general public via modem links.

[2] Study Material of Indian Law Institute, New Delhi, for PGDHR Course, p 3

result, activities which were earlier committed in physical space are replaced in cyberspace. Hence, new forms of crimes like- cyber defamation, cyber stalking etc., targeting the vulnerable sections of the society peeped into. Thus, cybercrime is a complex global phenomenon where interactions between people, software and services are supported by devices and networks for information as well as communication which have worldwide distribution. Now, do laws govern cyberspace or whether activities of internet are immune from any kind of regulation is often asked question.

A nation wise survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many of them have not even initiated steps to frame laws for policing against these crimes.[3] Here, an initiative has been taken to discuss the international as well as national laws as well as policy initiatives taken to curb the menace of cybercrime.

Cyber Crime: Theoretical and Conceptual Framework:

Cybercrime may be defined as a criminal activity that uses a computer either as an instrumentality, target or means of perpetrating further crime[4]. In other words, cybercrime is an unlawful act wherein the computer is either a tool or a target or both. These crime covers a wide range of illegal computer-related activities such as theft of communication service, dissemination of offensive pornographic materials in cyberspace, electronic vandalism etc.

Technical measures to protect computer systems are being implemented along with legal measures to prevent and deter criminal behavior. But 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 network is used as the source, tool or target is known Cybercrime.

The expression 'cybercrime' cannot be restricted only to hacking or planting computer virus into another's computer, but encompasses a wide range of crimes that use information technology in their commission or preparation. [5] These crimes cover a wide range of illegal computer related activities such as theft of communication services, cyber terrorism and extortion, tele-marketing frauds, illegal interception of tele-communication, dissemination of pornographic and offensive materials in cyber-space etc[6]. The common types of cybercrime may be discussed under the following heads: hacking, cyber stalking, cyber pornography, phishing, web jacking, software piracy, and cyber terrorism.

---

[3] *supra note 1*

[4] Prof. N.V. Paranjape, Criminology and Penology, Thirteenth Edition, 2008, pp. 133

[5] Dr AmitaVerma, 'Cyber Crimes in India,' First Edition, 2012 pp. Foreword

[6] Prof. N. V. Paranjape,, Criminology and Penology, Thirteenth Edition, 2008 pp.133

1.1 Concept of Cyber Law:

First coined by William Gibson[7], the term 'Cyberspace' is a popular descriptor of the virtual environment in which activity of internet takes place. The term cyberspace has become so popular that it seems to dominate the thinking of people who consciously or subconsciously feel that they are entering a place which has new meanings, dimensions and purposes. Internet has created new public spaces and communities. These spaces and communities are known as virtual because they are no longer linked with place or time.

Social interaction in cyber space is quite different from face to face environment. Geographical boundaries are transcended. Everything is recordable and no boundaries of "privacy" exist. Under complete anonymity, people become more disinherited than usual, or they might experiment with different identities. Sensory experience is expanded to multimedia experiences with highly creative fantasies. All these features of online space are characteristic of contemporary society i.e. network society.

2. Women in Cyberspace and Cyber Criminality:

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behavior. The World Wide Web (www) allows users to circulate content in the form of text, images, videos and sounds. Websites are created and updated for many useful purposes, but they can also be used to circulate offensive content such as pornography, hate speech and defamatory materials. The widespread circulation of such content is particularly harmful for women. The pervasive gender-discrimination in our society is further heightened since the digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behavior since it is presumed that they will not face any consequences. Furthermore, those who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cyber-stalking'. Women and minors who post their contact details become especially vulnerable since errant elements such as sex-offenders can use this information to target potential victims.

Furthermore, there is considerable social stigma which arises from the circulation of obscene images or videos or morphing of the images of women into pornographic content. Sometimes, women are forced to engage in sexual acts after being given threats that previously created images or videos will be circulated.

[7] William Gibon (1984), *Neuromancer*, pp. 4, Ace Hardcover, New York as accessed from URL: http://.www.cyber_Law_13245_09.html on 13th December, 2015 at 5 pm.

Such practices are a blatant invasion of privacy as well as an attack on an individual's dignity. Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. In India the term "cybercrime against women" includes sexual crimes and sexual abuses on the internet. Some of the crimes committed against women in cyberspace are: harassment via e-mail, cyber-stalking, cyber defamation, morphing, e-mail spoofing, hacking, cyber pornography and cyber sexual defamation, cyber flirting and cyber bullying etc.

Harassment via E-mail

Harassment via email is a form of harassment, which includes blackmailing, threatening, and constant sending of love-letters in anonymous names or regular sending of embarrassing mails to one's mail box.

Cyber stalking

This is one of the most popular internet crimes in the modern world. Cyber stalking can be defined as the repeated acts harassment or threatening behavior of the cyber-criminal towards the victim by using the internet services. Stalking in the internet happens when the perpetrator follows the victim continuously by leaving unwanted messages in cyberspace.

Cyber defamation

Cyber defamation occurs when with the help of computers and internet someone publishes derogatory or defamatory information to all of that person's friends or the perpetrator post defaming stories about the victim. Although this can happen to both genders, but women are more vulnerable.

Morphing

When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing.

Email Spoofing

E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields, ill-intentioned users can make the email appear to be from someoneother than the actual sender.

Hacking

Hacking means unauthorized access to computer system or network. It is an invasion into the privacy of data and it mostly happens in a social online community to demean a woman by changing her whole profile into an obscene, derogatory one. The reasons vary from personal hatred, revengeful mind to even just for fun.

Cyber Pornography
Internet may be considered the facilitator of crimes like cyber pornography; women and children are becoming the main victim of this flip side of technology.

Cyber sexual defamation
Cyber sexual defamation happens between real or virtually known people who out of frustration start publishing defaming stories in obscene languages on various social websites subsequently it turns into cyber pornography.

Cyber Voyeurism:
Voyeurism is the act of watching a person engaged in private activities. If a man watches or capture the image of a women engaged in private activities, when the women does not expect anyone to be watching, and disseminates such image is said to have committed the offence of cyber voyeurism.

Cyber flirting
Generally cyber flirting may be considered very minimal petty offence that starts when perpetrator force the victim to hear obscene songs, messages and it may consequently result in cyber sexual defamation and breach of thrust.

Cyber bullying
Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. The main aim and objective behind such crime may be to defame the target out of anger, hatred or frustration or secondly when the perpetrator wants to make simple fun of his friends, classmates, juniors or unknown net friends.

In **The United States v Lori Drew** (2006)[8] is one of the examples of cyber bullying. In this case a 13 year old girl got a message on Internet, "the world would be better off without you" and took it to her heart. She had not met the person who sent this message but only after twenty minutes she hung herself.

It is true that, other than cyber stalking, cyber pornography and morphing, men are equally susceptible to the other types of crimes mentioned here. But the majority of the victims of such offences are women as can be seen from the above study. Despite of that there is no separate provision for cybercrimes against women under Information Technology (IT) Act.

Factors for the growth of Cyber Crime against Women in India:
The reason for the increasing crime rate in cyberspace against women in India, even after the enactment of Information Technology (IT) Act, 2000 and its further

[8]URL: http://blog.koldcast.tv/2011/koldcast-news/8-infamous-cases-of-cyber-bullying/html as accessed on 10th November, 2015 at 4.00 pm.

amendment in 2008 cannot stop the sea growth of the crime rate against women in cyberspace can be categorized as under:

Lacunas in IT Act: The object of the IT 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. Majority of cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form), 72(breach of confidentiality).
Most of the cybercrimes other than e- commerce related crime are being dealt with these three sections. Cyber defamation, email spoofing, cyber-sex, hacking and trespassing into one's privacy is very common nowadays but IT Act is not expressly mentioning them under specific Sections or provisions. Indian constitution guarantees equal right to live, education, health, food and work to women. But the same modesty of women seems not to be protected in general except for Section 67[9].
(b) Jurisdiction Issues in Cyber related crimes: Transcendental nature of Internet is one of the main reasons for the growth of cybercrime. Whereas Section 75 of the IT Act deals with the offences or contravention committed outside India but it is not dealing with the jurisdiction of the crimes committed in the cyberspace especially the question of place for reporting the case when it arises or when the crime is committed in one place affected at another place and then reported at another place. Although in the most of the cases, for the matter of territorial jurisdiction Criminal Procedure Code is being followed.
(c) Sociological reasons: Most of the cybercrimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family's name. Many times she believes that she herself is responsible for the crime done to her. The women are more susceptible to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Although the women net surfers are very less in number as mentioned but the other groups targeting them above India, women still do not go to the police to complain against sexual harassment, whether it is in the real world or the virtual world they prefer to shun off the matter as they feel that it may disturb their family life.

4. Legal Mechanisms to deal with cybercrime against women in global context:

In UK, Cyber harassments and offences against women are comprehensively covered by the Protection of Harassment Act, 1997. The Act is considered more conservative to regulate gender centric Cyber harassment except those which involve physical harms. Harassment via e-mails and Cyber- stalking may be

[9] Section 67: Punishment for publishing or transmitting obscene material in electronic form.

considered some of the main offences against women in cyberspace. Hacking related activities may not always be restricted to crimes committed against the nation or the corporate entities alone but some time it may be seen as a crime when done to stored computer data or the computer as a machine of any female victim[10].

To access her personal information including pictures without proper authorization, with intention to misuse it, distribute it in the internet, modify the contents and give a false impression of the victims etc, are also criminal activities like stalking or bullying. Apart from Protection of Harassment Act, 1997 to cover cyber offences originating from domestic violence or dating violence, the offences related to unauthorized access are regulated by a compact legislation called " Computer Misuse Act, 1990".

This Act was created to protect the both men and women victims but the language clears that the Act suits to the need for preventive action against harassment of women. This Act mainly cover the three offences namely, unauthorized access to computer material, to enable any such access to secure unauthorized access, intention to create further menace with such unauthorized access and unauthorized modification of the computer material. The penalties for such offences are imprisonment for a term of 12 months or to a monetary fine not exceeding statutory maximum, or both.

USA is one of the countries which evaluated the dark and ugly side of internet; the cybercrimes. A study shows that till2010 among 349 victims 73 percent are women which evident the vulnerable condition of women in cyberspace[11]. Whereas it recognized protective laws at both level federal and state. USA noticed a hub of cases in the cybercrime against women and mitigates such crime to prevent future victimization.

Laws against sending obscene/ offensive material at Federal Level: Section 223(a) of Title 47 of the U.S. Code makes it an offense to use a telecommunications device in interstate or foreign communications to:
(1) make, create solicit and initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person";
(2) make, create solicit and initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene or

[10] Shobhna Jeet, Cybercrimes against women in India: Information Technology Act, 2000,Elixir International Journal, available online at URL: www.elixirpublishers.com as accessed on 11th November, 2015 at 7.30 pm.
[11] *Ibid*

indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication";
(3) Make a telephone call or "utilize a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications";
(4) Make or cause "the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number";
(5) Make repeated telephone calls or repeatedly initiate communication "with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication"; or
(6) Knowingly permit any telecommunications facility under his or her control to be used to commit any of the previously-listed activities.
The penalties for these offenses include fines, imprisonment for up to two years, or both.
Again, there is Privacy Act of 1974, which provides safeguards against invasion of personal privacy through the misuse of records by Federal Agencies. The Privacy Act holds that no agency should disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior consent of, the individual to whom the record pertains.
In case of other countries also cyber laws are being enacted looking at the propinquity of the crime rate and cybercrime. Even to tackle the complexities or problems of the virtual world universal codes like UNICTRAL laws has been passed basing on which separate legislations are introduced in the countries. These laws have often been described as 'paper laws' for 'paperless environment.'[12]

5. Laws to combat cybercrime against woman in India:
India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes. This Act 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 and children.[13] However there are few provisions to cover some of the crimes against women in cyber space under IT Act. The model adopted in USA may be proved a step forward in this direction.

[12] URL: http://www.lawctopus.com/academike/cyber-crimes-other-liabilities as accessed on 12/12/2015, at 3.30 pm.
[13] URL: http://www.genderit.org/es/node/2213) as accessed on 23rd November 2015 at 3 pm.

The Information Technology Act, 2000 (IT Act) was passed by the Indian Parliament in view of growing use of digital and internet technology in our country. This Act of 2000 is very unique in the sense that it deals with multiple issues under one umbrella for which separate legislations exist in different countries. By virtue of the provisions of the section 1 (2) and 75, the Act applies to any offence or contraventions committed outside India by any person irrespective of his nationality, if the act or contravention involves a computer or computer networks located in India.

The following sections of the Act of 2000 are applicable in case a woman is victimized in cyberspace.

Section 67: Publishing of Information which is obscene in Electronic form:
Whoever publishes or transmits or causes to be published in the electronic form any material which is lascivious or appeals to the prurient interest or if its effects is 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, shall be punished for the first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Further Section 66 A was inserted by the Information Technology amendment Act of 2008.
66A. Punishment for sending offensive messages through communication service, etc,:
Any person who sends, by means of a computer resource or a communication device any information that is grossly offensive or has menacing character; or 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 makes by making use of such computers resource or a communication device, or any electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or mislead the addressee or recipient about the origin of such message shall be punishable with imprisonment for a term which may extend to three years and with fine.

But this section has been declared unconstitutional by Hon'ble Supreme Court of India in 2015.[14]

[14] In the case of *Shryea Singhal v. Union of India,* on 24th March, 2015.

Besides the above provisions in the IT Act, provisions also exist in the Indian Penal Code 1860. The Criminal Law Amendment Act, 2013 inserted Section 354-D to the Indian Penal Code, 1860 to define and punish the act of stalking.

Section 354-D of IPC, 1860:
(1) Whoever follows a person or contracts 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 interfere with the mental peace of such person, commits the offence of stalking.

(2) Whoever commits the offence described in section 354-D (1) shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine. It is further provided that if a person commits the offence of stalking second time or again he shall be punished with imprisonment of either description for a term which may extend to five years and shall also be liable to fine.

In India, we don't have any specific legislation regarding cyber stalking. The Communication Conversion Bill, 2001 covers the case of cyber stalking. It is pending in the Parliament for its approval. Its clause 70 covers the case of Cyber stalking and is as follows:

Any person who sends, by means of a communication service or a network infrastructure facility,-
a. any content that is grossly offensive or of an indecent, obscene or menacing character; or
b. for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, content that he knows to be false or persistently makes use for that purpose of a communication service or a network infrastructure facility, shall be punishable with imprisonment for a term which may extend upon three years or with fine which may extend to rupees two crores or with both[15].

6. Present Scenario in India:
Most of the cases related to cybercrime against women reported to the police comes within the ambit of Section 67 (Publishing or transmitting obscene material in electronic form) of the Information Technology Act 2000 that is very much clear from the case study made from time to time and charges levied under section 506 (part II of the section which prescribes punishment for criminal intimidation to

[15]Justice Yatindra Singh, Cyber Laws, Second Edition, 2005 at p. 79

cause death or grievous hurt), 367 (which deals with kidnapping or abduction for causing death or grievous hurt) and 120-B (criminal conspiracy) of the IPC and Section 67 of Information Technology Act, 2000 (which dealt with obscene publication in the internet).

Some of the applications of law on the basis of the crime committed against women are brought hereunder:

Harassment via E-mail: Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cybercrime. After the amendment in 2008 new Sections have been inserted as Section 67 A to 67 C Section 67 A and 67 B insert penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 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. These provisions in general are used to book the perpetrators along with Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman.

In such cases the victim goes to the police station to report the crime of harassment and thereby it is regulated as per the general laws and not by the provisions of cyber laws.

Cyber stalking: Similar to the case of email harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the IT Act that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women.

Cyber defamation: As cyber defamation is not defined by the IT Act 2000 therefore, it is treated by the criminal justice system under the same provisions of cyber pornography or publication of obscene materials in the internet (Section 67 of the IT Act 2000). The offence is well explained in the IPC under Section 500 which mentions punishment with simple imprisonment which may extend to two years or with fine or with both; and under Section 501 which states that “whoever prints or engraves any matter, knowing or having good reason to believe that such matter is defamatory of any person, shall be punished as per Section 500”.

Hacking: Morphing, hacking, and email spoofing are interrelated and attract Sections 43 (penalty for damage to computer, computer system etc.) and 66 (hacking of the computer system; first proviso to the said section states that

whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value, its utility or affects injuriously by any means, commits hacking) of the IT Act 2000. The perpetrator can also be booked under the IPC for criminal trespass under Section 441, Section290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation.

Cyber Pornography: Unlike other crimes like Cyber Stalking, Cyber Defamation, Morphing, Email Spoofing, Cyber Pornography is considered an exceptional case which has been covered by the IT Act 2000 to a certain extent by Section 67 of the IT Act 2000. Along with IT Act the perpetrator can be punished under various Sections of IPC (Section 290 for committing public nuisance, section 292for sale of obscene books etc, and section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, section 293 for sale etc., of obscene objects to young persons and then section 294 for doing or composing, writing etc., of obscene songs and finally under section 509 for outraging the modesty of women).

Cyber sexual defamation: The accused can be booked under section 67 and 72 of the IT Act as well as IPC.

Cyber flirting: For cyber flirting, except Section 72 which deals with the breach of confidentiality and privacy there is no other support that can be offered by the Act to the victim.

Under Section 354 C the term 'Voyeurism' was introduced in the Indian Penal Code, 1860 by the Criminal Law (Amendment) Act, 2013. The provision holds that if any man who watches, or captures the image of a women engaging in a private act in circumstances that she would usually have the expectation of not being observed either by the perpetrator or any other person at the behest of the perpetrator or disseminates such image shall be punished on the first conviction with imprisonment for either description of a term which shall not be less than one year, but which may extend to three years or shall be liable to fine, and shall be punished on second or subsequent conviction, with imprisonment for 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.[16]

Again, the Privacy (Protection) Bill, 2013is yet to see the light of the day, as it is pending in the Parliament. Although this Bill does not provide any definition of

[16] The Criminal Law (Amendment) Act, 2013.

privacy, however, it focuses on the protection of personal and sensitive personal data of persons.

7. Conclusion and Suggestions:

Cybercrime is a global menace as it targets and even affects the person far away from the place of offence, may it be in the same country or some other country. Looking at the sea growth rate of cyber related crimes especially against women, it can be firmly said that policing at international level as well as active cooperation between international community and the nations are the foremost requirement of the hour. It has been seen that although various laws, rules and regulations both in national as well as international forum are there, but still fencing this borderless crime has become difficult. Women who are harassed and abused in cyberspace are often seen to be reluctant to seek legal help and often choose to move back which gives the perpetrators another chance to ruin their lives. The probable reason may be social or personal inhibition or may be losing faith in legal remedies provided to them. Even what is more shocking is that till date both in national as well as international forum, there is no law in force which specifically provides for protection of women in cyberspace. Besides law and legal institutions, the solution to the problem of abuse and harassment need to be searched in the societal norms and values and the willingness of the professionals and activists[17] to curb this menace.

In order of the discussion made here above, the author would like to give some suggestions which are as follows:

1. Need of a Universal Model Charter on cyber law specifically dealing with women: There is need of a Model Charter to prevent further victimization of women in cyber world by providing firstly specific definitions on various cybercrimes committed against women, then on providing a code of conduct applicable to both the sex and thirdly, provide mechanisms to spread awareness about cyber related crimes as well as laws.

2. Assert the applicability of legal norms across national borders: Although it is said that internet is a regulation free zone, but in fact there is plenty of regulations for the internet, however not enough to protect the privacy of its inhabitants. Users of the internet have at least as much right to claim a legal right to protect their personality.

3. Promote the development of technology to protect privacy: To ensure effective application of privacy rights across borders is must, but here we must not ignore the possibility that technology may provide some solutions to the protection of

[17] URL: www.unesco.org-papers-paper_10 as accessed on 12th October, 2015, at 6.45 pm.

privacy. Here again, we should be careful enough to distinguish between the means that in fact protect privacy and those that merely appears to.

4. Coordination between Government and Other Agencies: To combat cybercrime, concerted coordination and action between governmental and non-governmental actors, including educators, health-care authorities, legislators, the judiciary and the mass media is required *in toto*. Training to handle cyber related crimes must be incorporated in the governments agenda, and police personals, magistrates, media etc. are to be trained accordingly.

5. Organizing workshop, Seminar, Conference etc.: Workshops, Seminar, Conference etc., must be held from time to time by the activist as well as academic institutions so as to discuss the issues related to women in cyberspace. NGO's as well as Legal Aid Clinics in Law Schools may also take the lead by awaking the masses specially women through awareness camps, street plays, distributing pamphlets etc. dealing with the issues as to what amounts to infringement of privacy rights in cyberspace, what a victim of cybercrime use to do, remedies provided by law etc. It will not only help in changing the attitude of the victim towards herself but also of the society as a whole towards the victim.

It must be noted here that law is not the only solution to every problem. Mere law making will not suffice if attitudinal changes are not accomplished with. However, we cannot negate the role of law. Laws are must, but law must pace with the society. Thus, along with seeking solutions through law, social solutions are also to be given due importance. If any law or policy is superficially made where patriarchal syndrome still exist, then to consider such policy to serve any purpose is a myth.

Let us enjoy the benefits of the future while preserving the freedoms, values, ethics, and morality of our past.

REFERENCES

Amar, Meena(2011) Lectures on cyber laws, Asia Law House, Hyderabad, First Edition.

Criminal Law (Amendment) Act, 2013

Indian Penal Code, 1860

Information Technology Act, 2000

Kamath, Nandan(2012) Law Relating to Computers Internet & E-Commerce- A Guide to Cyberlaws & The Information Technology Act, Rules, Regulation and Notifications along with latest case laws, Universal Law Publishing Company Pvt. Ltd., New Delhi, Fifth Edition.

Paranjape, Prof. N.V, Criminology and Penology, Central Law Publications, Allahabad, Thirteenth Edition, 2008, p. 133

Ryder, Rodney D.(2001) Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet), Wadhwa and Company Law Publisher, Delhi, First Edition

Singh, Justice Yatindra(2005) Cyber Laws, Universal Law Publishing Co. Pvt. Ltd, Delhi, Second Edition,
Study Material of Indian Law Institute, New Delhi for Online course in Cyber law.
Study Material of Indian Law Institute, New Delhi, for PGDHR course.
Verma, Dr. Amita, Cyber Crimes and Laws, Central Law Publications, Allahabad, First Edition, 2009.
Verma, Dr. Amita, Cyber Crimes in India, Central Law Publications, Allahabad, First Edition, 2012
Verma, S.K & Mittal, Raman (edited), Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, Edition 2004.

Internet Sources:

URL: http://.www.cyber_Law_13245_09.html as accessed on 13th December, 2015 at 5 pm.
URL:http://blog.koldcast.tv/2011/koldcast-news/8-infamous-cases-of-cyber-bullying/html as accessed on 10th November, 2015 at 4.00 pm.
URL: www.elixirpublishers.com as accessed on 11th November, 2015 at 7.30 pm.
URL: http://www.lawctopus.com/academike/cyber-crimes-other-liabilities as accessed on 12/12/2015, at 3.30 pm.
URL: http://www.genderit.org/es/node/2213) as accessed on 23rd November 2015 at 3 pm.
URL: www.unesco.org-papers-paper_10 as accessed on 12th October, 2015, at 6.45 pm.