Women: A Victim of cyber crime

Anupama Singh
Research Scholar
Faculty of Juridical Sciences
University: Rama University,Kanpur

Dr. Praveen Kr. Mall
Assistant Professor
Faculty of Juridical Sciences
Rama University,Kanpur

"There are important gender differences when it comes to cyber crime victimization. Males are more likely to commit offences, while females are more likely to be victimized"

Debarati Halder.[1]

INTRODUCTION

Cyber crime against women in India is relatively a burning and recent concept. It can be noted that when India started her journey in the field of Information Technology, the instant need is to protect the electronic commerce and related communications and not cyber socializing communications. The drafters of the Indian Information Technology Act, 2000, make it on the influence of the Model Law on Electronic Commerce, which was implemented by the resolution of the General Assembly of the United Nations in 1997[2]. The Act turned out to be a half baked law as the operating area of the law goes beyond electronic commerce to cover cyber attacks of non-commercial nature on individuals as well. While commercial crimes and economic crimes were somewhat managed by this Act, it miserably failed to prevent the growth of cyber crime against individuals, including women. However, it took nearly eight years for the Indian Parliament to create a modified all exclusive information technology law which tries to control illegal cyber activities with major focus towards protection of electronic commerce. During this break of eight years of the perplexed lawless circumstances, India witnessed growth of cyber crimes and watched helplessly the perpetration of cyber crime against women in particular. Often the laws that were used to combat such crimes set a wrong example and confusion, women victims were extremely discouraged to report the crimes by peers, immediate media attention and the attitude of perplexed government reporting agencies made women victims more disturbed than their cyber crime victimization.

[1] *Risk behaviours increase exposure to cyber crimes* (, 2016) available at http://www.criminologysymposium.com/symposium/event-information/2016archive/news/-risk-behaviours-increase-exposure-to-cyber-crime.html..

[2] Prof. Dr. Marco Gercke , *Understanding Cybercrime: Phenomena, Challenges And Legal Response* (2012) available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

The reason for the increasing cyber crime rate against women is that most of the cyber crimes stay 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 vulnerable to the risk of cyber crime as the perpetrator's identity remains unidentified and he may constantly threaten and blackmail the victim with different names and identities. Women still do not go to the police to complain against perpetrators so, the problem would be resolved only when the victimized woman immediately report back or even warn the abuser about taking strong actions.

There are different kinds of cyber crimes which can be committed against person or individual, organization or government and it may be against the society at large but, in this paper the focus is only on cyber crimes against women. It is because more than the financial loss, injury to the reputation and honour of the person or individual is important to the victims of cyber crime, particularly when the victims happen to be a women.

Cyber Crime against Women

Cyber crime against women in India was an issue of which few talked about and few worked on and which was suffered by enormous numbers of victims helplessly. The term 'cyber crime against women' in India is mainly cover sexual crimes and sexual abuses in the internet, such as morphing the picture and using it for purposes of pornography, harassing women with sexually blackmailing / harassing mails or messages etc, or cyber stalking. This is also evident from the fact that majority of the cases reported to the police are of the nature of sexual crimes and most of them are booked under the erstwhile Section 67 (which was meant to cover pornography and obscenity in the internet) of the Information Technology Act, 2000).[3]

Types Of Cyber Crime Against Women

Amongst the various cyber crimes committed against individuals and society at large here are few basic cybercrimes that mainly happens to women in India in the cyberspace such as harassment via e-mail, cyber stalking, cyber defamation, morphing, email spoofing and cyber pornography. These different types of cyber crimes against can be discussed briefly as follows[4]:-

[3] Debarati Halder & K. Jaishankar, *Cyber crime and the victimization of women: laws, rights and regulations* (2012), USA, Information science reference, P. 113.

[4] Dhruti M Kapadia, Cyber Crime Against Women And The Laws In India (2018) **https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/** https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/

i) Cyber stalking

This is one of the most famous about internet crime in the modern world cyber stalking. The University of Virginia defines stalking as behaviour wherein an individual wilfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, tortures or intimidates that person. It is the frequent acts of harassment or threatening behaviour of the cyber criminal towards the victim by using the internet services. Stalking in the internet happens when the perpetrator follows the victim constantly by leaving unwanted messages. The motivation of stalkers may be considered less than four reasons, (i) sexual harassment, (ii) obsession for love, (iii) revenge and hate, (iv) ego and power trips. The stalker disturbs their targets through private emails as well as public message.[5]

ii) Harassment via E-mail

Harassment via email is a sort of harassment, which includes blackmailing, threatening, and continuous sending of love letters in unspecified names or continuous sending of embarrassing mails. Criminal Procedure Code, Indian Penal 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 way and format as the central government may prescribe. These provisions do not mention anything about e-mail harassment of different type but in general they are used to book the perpetrators along with Section 292A of the IPC 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. The issues related to publication or transmission of obscene information in electronic form under Section 67 of IT Act 2000 may be looked from the perspective of 'extraterritorial' jurisdiction.[6]

iii) CYBER BULLYING

Today, people all over the world have the capability to communicate with each other with just a click of a button and technology opens up new risks. Cyber bullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else Cyber bullying is "willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature. "Globally, India is third behind China and Singapore in cyber bullying or called online bullying Cases of suicides linked to cyber bullying have grown

[5] Debarati Halder, *Cyber Crime against Women in India, available at* URL: http://www.cyberlawtimes.com/articles/103.html,.
[6] Bhupinder Jit Kaur, *Cyber Crimes against Women in India: Information Technology Act, 2000* (2013), available at URL: http://www.ssmrae.com/admin/images/c2b97adc889cddc715acbd682d2757bf.pdf, Pp. 19-20.,.

over the past decade.[7] Bullying classmates, juniors or even seniors in the school is a common culture among the young school students in India Social networking sites used in nearly half of cases[8].

iv) Cyber defamation

Cyber defamation happens 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, women are more vulnerable.[9]

Unfortunately cyber defamation is not defined by the IT Act 2000 and it is treated by the criminal justice system under the same provisions of cyber pornography or publication of obscene materials in the internet[10]. The offence defamation is well defined in the IPC under Section 500 ".[11]

v) Cyber Pornography

Internet may be considered the facilitator of crimes like cyber pornography; women and children are becoming the main victims of this flip side of technology.[12]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[13]

vi) **Email spoofing**

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates.[14]The more common method used by men is to email offensive photographs of themselves to women, praising their beauty, and asking them for a date or inquiring how much they charge for 'services'. Besides sending explicit messages via e-mail, SMS and chat, many also morph photographs - placing the victim's face on another, usually nude, body[15].

vii) Morphing

[7] Childnet International "Cyberbullying: A whole-school community issue" available at http://digizen.org/downloads/cyberbullyingOverview.pdf
[8] *Published on* Do Something "11 Facts about Cyber Bullying" available at http://www.dosomething.org/tipsandtools/11-facts-about-cyberbullying
[9] Supra note 10, P.3.
[10] .Section 67 of the IT Act 2000
[11] Supra note 8, P. 8893.
[12] Supra note 19.
[13] Section 290 for committing public nuisance, section 292 for 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).[13]
[14] Supra note 19.
[15] Ibid.

Morphing is editing the original picture by unauthorised user or fake identity. It was identified that female's pictures are downloaded by fake users and again re-posted or uploaded on different websites by creating fake profiles after editing it. This amounts to violation of I.T. Act, 2000 and attracts Sec. 43 & 66 of the said Act. The violator can be booked under IPC also.[16]

Legal Provisions Relating to Cyber Crime against Women In India

Information Technology Act, 2000:

i. **Section 66- Computer related offence:** Under this section, if anyone, dishonestly or fraudulently, does any act referred to in Section 43 of the IT Act, 2000, he or she shall be punishable. In other words, to be charged under section 66, any person must cause a computer resource to perform a function with dishonest or fraudulent intent to secure access, knowing that the access he intends to secure is unauthorized.[17]

It involves an invasion of right and diminution of the value or utility of one's information residing in computer resources. The accused must have contemplated this when he committed such an offence against a computer resource. Computer related offence involves mental act with destructive animus.[18] While deliberating upon such cases, one should not disregard the fact that proving destruction or alteration of data attached to an identifiable, tangible property would not only be highly technical but may also bring an undesirable degree of uncertainty in the operation of law.[19]

The legislative intent behind importing these two sections from the IPC is to introduce the component of *mens rea*. Here, the offence depends upon intention, i.e., whether the act is done 'dishonestly' or 'fraudulently'. The criminal intent in computer related offence manifests itself in terms of causing wrongful loss or damage as it has been defined under section 23 of the IPC.[20]

(ii) Section 66 A :

This section creates an onus on the sender of the message, not to send any message by means of a computer resource or a communication device which may be Grossly offensive, Known to be false, Cause annoyance.[21]Such messages can be in the form of text examples e-mails, SMS, blogs, blogs, tweets, image, sound, voice over Internet Telephone services like Skype, Google talk etc..

[16] Supra note 7, p.3.
[17] Vakul Sharma, *Information Technology Law and Practice*, 3rd Ed, New Delhi, Universal Law Publishing Co. (2011), P. 174.
[18] Supra note 29, P. 174.
[19] Supra note. 29, P. 177.
[20] Ibid.
[21] Ibid P. 182.

(iii) Section 66 E- Punishment for violation of privacy[22]

If anyone by his or her act fulfills the above ingredient, he or she is said to be liable for the violation of the privacy of that person. The instances of violation of privacy includes installation of hidden cameras, spy cams or any communication device inside the restrooms, bedrooms, changing rooms, hotel rooms etc. for the purpose of violating bodily privacy of any user or occupant of such places.[23]

Sting operation by a private person or an agency, which may result in violating bodily privacy of another person, will fall under Section 66E of the Act. Whatever may be the reason- public interest or the people's right to know, one should not disregard the protection being given to an individual against his bodily privacy.[24]

In ***Court on its own motion v. State,***[25] the Division Bench of the Hon'ble Delhi High Court summarized its views on sting operation by stating that, any sting operation, if it violates bodily privacy of another person, such a private person or agency conducting any such sting operation would be making itself liable for action at law[26].

(iv) Section 67- Punishment for publishing or transmitting obscene material in electronic form[27]

The section advocates that the 'obscene material in electronic form' must be considered by itself and separately to find out whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the 'obscene material in electronic form' is likely to fall.[28]

[22] The essential ingredients under this section are as follows:[22]Any one intentionally or knowingly, Captures, publishes or transmits any image of a private part of any person, Without the person's consent

[23] Ibid.

[24] Ibid.

[25] WP (Crl) No. 796. (2007).

[26] A sting operation by a private person or agency is, by and large, unpalatable or unacceptable in a civilized society. A sting operation by a State actor is also unacceptable if the State actor commits an offence so that an offence by another person is detected.A State actor or a law enforcement agency may resort to hidden camera or sting operations only to collect further or conclusive evidence as regards the criminality of a person who is already suspected of a crime. The law enforcement agency must maintain the original version of the actual sting operation. Tampering with the original video or audio clips of a sting operation may lead to a presumption of the spuriousness of the entire operation. A sting operation cannot be initiated to induce or tempt an otherwise innocent person to commit a crime or entrap him to commit a crime. Normally, if a private person or agency unilaterally conducts a sting operation, it would be violating the privacy of another and would make itself liable for action at law. A sting operation must have the sanction of an appropriate authority. Since no such authority exists in India, and until it is set up, a sting operation by a private person or agency, ought to have the sanction of the Court of competent jurisdiction which may be in a position to ensure that the legal limits are not transgressed, including trespass, the right to privacy of an individual or inducement to commit an offence etc.

[27] The ingredients of offence under this section are: Publication or transmission in the electronic form, Any material lascivious or appeals to the prurient interest, Tendency to deprave and corrupt persons, Likely audience, To read, see or hear the matter contained or embodied in electronic form.

[28] Ibid.

Critically speaking, the aforesaid section, like section 292(1), IPC, does not make knowledge of obscenity an ingredient of the offence. Thus to escape criminal charges, one has to prove his lack of knowledge of publication or transmission of obscene information in electronic form..[29]

Another missing link in the section has been the lack of exceptions as detailed in section 292, IPC, i.e., the exceptions which are available on account of public good, religious purposes, etc. may not be available if such publication or its transmission is in the electronic form.[30]

(v) Section 67A- Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form[31]

It is significant to note that publication or transmission in the electronic form includes dissemination of information or data in electronic form.[32] In view of the ease with which obscene content can be replicated, misused, and distributed over the internet using all kinds of information technology and communication tools- it was felt by the lawmakers to move beyond 'likely audience" test of section 67 and provide more stringent mechanism to combat obscenity in electronic form.[33]

The amendment Act has incorporated the *Exception* as provided under section 292 of IPC as proviso in the sections 67 and 67 A.[34]The issue related to publication or transmission of obscene information in electronic form has to be also looked from the perspective of 'extra- territorial' jurisdiction and internet technologies, keeping in view that 'obscenity' is no longer a local and static phenomenon. It is now global and dynamic in nature and thus needs strict interpretation of statute.[35]

[29] Ibid.
[30] Ibid.
[31] The ingredients of offence under the aforesaid section are:[31]Publication or transmission in the electronic form, Any material containing sexually explicit act or conduct.

[32] Ibid P. 202.
[33] Ibid.
[34] Ibid.
[35] If any man who: Follow a woman and contact, or attempt to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman Monitor the use by a woman of the internet, email or any other form of electronic communication

Offences Relating To Women under Criminal Law Amendment Act 2013

1. **Section 354 D- Stalking**

This section has been inserted by the Criminal Law (Amendment) Act, 2013 and it includes all kinds of stalking including cyber stalking committed against the women. The following are the ingredients of this section:[36].

There are exceptions to this section which include such act being in course of preventing or detecting a crime authorized by State or in compliance of certain law or was reasonable and justified.

2. **Section 416 Cheating by Personation**[37]

Anyone pretends to be someone else than his real self, by word, act, sign, or dress, the offence under this section is committed provided some gain has accrued or some loss. Personation by itself is no offence but when a person fraudulently and dishonestly does a fraudulent act and represents as if he is himself that other person, section 416 will be attracted. Regarding cyber crime against person or individual like email spoofing can be booked under this section.

3. **Section 469- Forgery for the purpose of harming reputation**

Forgery for the purpose of harming the reputation of any party has been made punishable under this section.[38] The section stipulates that forgery must be committed and the offender must have the requisite intention or knowledge as indicated by the section.

In the case of ***State of Tamil Nadu v. Suhas Katti*** [39], the case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group.

However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

4. **Section 499-** deals with defamation which also has 11 exceptions. There are three ingredients under this section which are as follows: [40]

The Supreme Court in ***Benett Coleman & Co. v. UOI,*** [41] defined publication means dissemination and circulation. The IPC by 'signs' or 'visible representation' includes defamation in electronic form e.g.

[36] Criminal Law (Amendment) Act, 2013, available at: http://indiacode.nic.in/acts-in-pdf/132013.pdf.
[37] To fall under this section the accused should fulfill the following ingredients:[37]Pretending by a person to be some other person; Knowingly substituting one person for another; and Representation that he or other person is a person other than he or such other person really is.

[38] The ingredients of the section are as follows: The document or electronic record in question is forged; The accused forged it; The document or electronic record would be to defame or harm the reputation of someone.
[39] Decided on 2004 available at url: http://delhidistrictcourts.nic.in/CYBER%20LAW.pdf
[40] Section 499, Indian Penal Court, 1860.

generating, sending or receiving 'defamatory' emails online, bulletin boards messages, chat room messages, music downloads, audio files, screaming videos, digital photographs, etc., on internet. Even sending 'defamatory' sms, mms, photographs and videos on mobile phones is also an offence.

In ***P. Lankesh v. H. Shivappa,*** [42] it was decided that defamation takes place where the imputations are read on internet the place where the imputations are downloaded, publication takes place..

The immunity is granted to ISP is absolute if and only if he proves for any third party information that:

(1) He had no knowledge that the information content it is transmitting is unlawful or
(2) He had exercised all due diligence to prevent transmission (or publication) of unlawful content.

In ***K. Narayanan v. State,*** [43] the Supreme Court said that "the freedom of speech and expressions guaranteed by Art. 19(1) (a) included the freedom to acquire knowledge to read books and periodicals and read any type of literature subject only to reasonable restrictions being placed on such rights."

This fundamental right also extends to internet medium and every citizen has freedom to share, acquire knowledge by using internet and other resources subject to reasonable restrictions that is decency and morality.

Contravention is generic while offence is specific. Cyber crime-encompasses both cyber contraventions and cyber offences. Cyber word also includes computer, computer system, or network. Cyber crime must include *men rea*

1) Intent secure unauthorized access and
2) Knowledge that *actus reas* is unauthorized

4. Criminal intimidation[44]

In criminal intimidation, the immediate purpose is to induce the person threatened to do or not to do, or to obtain from doing, something which he was not legally bound to do or to omit[45]. Thus the section has the followings ingredients:[46]

[41] (1972) 2SCC 788.
[42] (1994) Cr. L. J. 3510 (Kant).
[43] (1973) A. Ker 97 (FB).
[44] Section 503, Indian Penal Code, 1860..
[45] Threatening a person with injury:To his person, reputation, or property, or To the person, or reputation of anyone in whom that person is interested;Threat must be with intent: To cause alarm to that person, or, To cause the person to do any act which he is not legally bound to do as the means of avoiding the execution of such threat, or To cause that person to omit to do any act which that person is legally entitled to do as the means of avoiding the execution of such threat

[46] Supra note 65, P. 826.

Cyber stalking or harassment via email in effect is committing criminal intimation with the help of computers. The offender might be causing alarm by sending messages via the internet to the victims threatening injury to him or her, his or her property or reputation. The computer is merely used as a tool for committing the offence and to be able to more effectively threaten his victim. The anonymity over the internet gives the offender a suitable shield to commit the offence without being easily detected. However, the end- result being the same, cyber stalking or harassment via email is merely criminal intimidation under section 503 of the IPC.

Outraging the Modesty of A Woman[47]

The object of this section is to protect the modesty and chastity of a woman.[48]When an accused sent a letter containing indecent overtures, lewd and filthy suggestion to an unmarried nurse, it was held that he has committed an offence under this section,[49] Therefore, the above are the legal provisions dealing to cyber crimes under Indian law with special reference to women in which we can understand that cyber crimes can be booked under Information Technology Act as well as under Indian Penal Code.

Unfortunately Chapter XI of the IT Act deals with the offences still needs to be modified. It does not mention any crime specifically as against women. Again, no section in the IT ACT 2000, states that personal viewing of obscenity an offence, in fact like in IPC Section 292 again, if it is proved that you have published or transmitted or caused to be published in the electronic form only then under Section 67 it can be an offence. Last but not the least, the IT Act, 2000 does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing as offences.

REMEDIES AVAILABLE TO VICTIMS OF CYBER CRIME

The legal provisions and the remedies available for the victims of cyber crime under IT Act and the punishments for the offenders under Indian laws has been analyzed.

Remedies for victims of cyber crime under Information Technology Act, 2000:

Under the Information Technology Act the remedies available for the victims of cyber crime are civil in nature. The consequences of sections 43 and 45 of earlier IT Act were Civil in nature having its remedy in the form of damages and compensation only, but under Section 66 of the IT Amendment Act, if such act is done with criminal intention that is *mens rea*, then it will attract criminal liability providing imprisonment or fine or both to the offender.

[47] Section 509, Indian Penal Code, 1860.

[48] The following essentials ingredients, viz Intention to insult the modesty of a woman; The insult must be caused- By uttering word, or making sound, or gesture or exhibition any object so as to be heard or seen by such woman, orBy intruding upon the privacy of such woman P. 833.

[49] *Emperor v. Tarak Das Gupta,* AIR 1926 Bom. 159.

By virtue of section 43[50], the following acts, if done without permission of the owner or any other person who is in charge of a computer/ network, etc., are contraventions-[51]The person contravening any of these clauses will be liable to pay the damages by way of compensation to the person so affected.

Section 45 provides residuary penalty for the IT Act or any rule of regulation there under[52]. The section is attracted when there is a contravention of provisions of the IT Act or any rules or regulations for the contravention. The section provides for the payment of penalty for such contravention or compensation to the person who has been affected by such contravention for a sum not exceeding twenty five thousand rupees.[53]

Punishment of the Offender of Cyber Crime under Information Technology Act, 2000:

i. **Section 66:**

Under this section, if any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or both.[54]. In other words, to be charged under section 66, any person must cause a computer resource to perform a function with dishonest or fraudulent intent to secure access, knowing that the access he intends to secure is unauthorized.

ii. **Section 66A:** If any person sends any message by means of a computer resource or a communication device which may be grossly offensive, Known to be false Cause annoyance or inconvenience to the recipient.[55]He or she shall be punished with imprisonment for a term which may extend to three years and fine.

[50] Accessing or securing access to the computer/ network or computer resources; Downloading any data or information from the computer/ network; Introducing or causing to be introduced any computer contaminant or computer virus into the computer/network; Damaging or causing to be damaged the computer/network, data, computer database or any other programmed residing in it; Disrupting or causing the disruption of the computer/network; Denying or causing the denial of access to any person authorized to access the computer/ network by any means; Providing assistance to any person to facilitate access to the computer/network in contravention of the provisions of the Act, rules or regulations made there under; Charging the services availed of by a person to the account of another person by tampering with or manipulating any computer/network; Destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means; Destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means. Stealing, concealing, destroying or altering or causing any person to steal, conceal, destroying or alter any computer source code used for the computer resources with an intention to cause damage.[50]

[51] Nanda Kamath, *Computers Internet and E- Commerce: A guide to Cyber laws and E- Commerce*, 4th Ed, New Delhi, Universal Law Publishing Co. Pvt. Ltd. (2009), P. 228.
[52] Section 45, IT Act. 2000.

[53] *Ibid,* P. 541.
[54] *Ibid,* P. 546.
[55] *Ibid.* P. 547.

iii. **Section 66 E:** This section provides punishment for violation of privacy and if any person is found that he or she a) intentionally or knowingly, b) captures, publishes or transmits the image of a private area of any person, c) without his or her consent, violates the privacy of that person he or she will be punished with imprisonment which may extend to three years or fine not exceeding two lakh rupees, or with both.[56]

iv. **Section 67:** This section provides punishment for publishing or transmitting obscene material in electronic form. If anyone does this act he or she will be punished on 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 with fine which may extend to ten lakhs rupees.[57]

In ***Dr. Prakash v. State of Tamil Nadu,*** [58] the offender was charged under section 506 (part II of the section which prescribes punishment for criminal intimidation to 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). He was sentenced for life imprisonment and a pecuniary fine of Rupees 1, 25,000.

v. **Section 67A**[59]**:** This section provides punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. If anyone committed this act shall be punished on the first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which extend to seven years and fine which may extend to ten lakh rupees.[60]

Punishment under Indian Penal Code, 1860

i) **Section 354D**[61]**:**

This section has been recently inserted by the Criminal Law (Amendment) Act, 2013 and it includes cyber stalking committed by a man to a woman and it provides punishment on the first conviction with imprisonment of either description of either description for a term which may extend to three years and shall

[56] Ibid P. 548.
[57] Ibid. 549.
[58] Supra note 56.
[59] Inserted by Information Technology (Amendment) Act, 2013

[60] Supra note 75, P. 549.
[61] Inserted by Criminal Law (Amendment) Act, 2013.

also liable to fine; on second or subsequent conviction, with imprisonment of either description for a term which may extend to five years and also liable to fine.[62]

ii) Section 469:

This section punishes anyone who commits forgery for the purpose of harming the reputation of any party and if anyone committed this act has been made punishable with imprisonment of either description for a term which may extend to three years and shall also liable to fine. [63]

In the case of ***State of Tamil Nadu v. Suhas Katti,*** [64] " The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay a fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year simple imprisonment and to pay a fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay a fine of Rs.4000/- All sentences to run concurrently."

iii) Section 500:

This section provides punishment for anyone who committed defamation and if anyone found that he defames another shall be punished with imprisonment for terms which may be extend to two years, or with fine, or with both.[65]

iv) Section 509:

Under this section, the law provides punishment for anyone who is intending to insult the modesty of any woman, utters any word or sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which extend to one year, or shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.[66]

Therefore, the remedies available to the victims of cyber crime by way of compensation are limited. Only a few sections in the IT Act i.e., sections 43 and 45 provide remedies in general to all victims of cyber crime and not specifically to women victims. However, many sections in the IT Act deal with increased punishments to the offenders and imposition of huge fine ranging ten thousand to one Crore. Unfortunately, even this fine amount imposed on the offender under the law do not go to the victims of cyber crime, as there is no mention of it in the legal provisions.

[62] Supra note 64.
[63] Indian Penal Code, 1860.
[64] Supra note 67.
[65] Supara note 89.
[66] Ibid.

It is recommended that the law makers should review these provisions and make the fine amount collected from the offenders go to the respective victims as compensations to heal the injuries of loss of personal reputation and several consequences in their future life. Thus, the punishment prescribed under the IT Act does not help the victims of cyber crime in any way, unless more remedies in the form of compensation and restitution are provided to the victims.

CONCLUSION

Internet is a medium and every citizen has freedom to share, acquire knowledge by using internet and other resources. But, some people who used internet users misuse it and commit a crimes using internet. Most of the cyber crimes committed against the person or individual are committed against women and hence in this category of cyber crime there are more women victims than men victims.

Cyber crimes against women can be booked under IT Act as well as IPC. India is one of the few countries to enact IT Act to curb cyber crime. Unfortunately the Chapter XI of the IT Act deals with all cyber offences and it does not mention any crime specifically against women it is a lacuna that the IT Act, 2000 does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing as offences even though it has been amended in the year 2008. The model adopted in USA may be proved a step forward in this direction.

However, the remedies available to the victims of cyber crime by way of compensation is limited to a few Sections in the IT Act, e.g. many sections in the IT Act provides punishments for the offenders and imposition of huge fine, but it does not benefit the victims of cyber crime in any way.

SUGGESTIONS

An analysis of the IT Act, 2000 reveals that there are no specific provisions which deal with cyber crimes against women exclusively or separately. Even the remedies available for the victims of cyber crime are limited and do not deal with women victims specifically. Thus, following recommendations have been made to improve justice to women victims of cyber crimes:-

1) There is a need for modification of IT Act as it does not mention any crime specifically as against women and secondly, it does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing etc as an offence.
2) Women are still not open to report cyber crimes against them which have been committed against them and this provides a chance for offenders to escape after the commission of cyber crime. In order to solve this

problem women victim should be encouraged to report their victimization to the police by creating more awareness among the women[67].

3) Judiciary plays an important role to deal with cyber offenders and at present the judges handling these types of specialized crime do not have expert knowledge in this field. To improve the situation, there should be more training programmes on cyber crimes to the judicial officers so that they can handle the cases in a better way. The judges also should have more sensitivity towards women victims of cyber crime as in this crime when the women come to the court as victims or witnesses; they need to be handled with dignity and respect by the Court officials.

4) The framers of the law may also consider the gravity of victimizations suffered by the cyber crime victims not only in the case of financial crimes, but also in the case of crimes against the reputation of the persons particularly the women victims and the fine imposed on the offender should be granted as restitution/ compensation to the victims[68].

REFERENCES

A. Books/Journals

1. Adam, A. (2001). Cyber Stalking: Gender and Computer ethics. In E. Green & A. Adam, Virtual gender: Technology, Consumption and Identity. London: Routledge.

2. Alexy, E., Burgess, A.W., Baker, T. &Smoyak, S. (2005). Perceptions of cyberstalking among college students.Brief Treatment and Crisis Intervention, 5, 279-289.

3. Arora, Sanjay. (2007). Stress on combating cyber crime, Violence against women. Retrieved on 11th Feb 2013 from http://www.hindu.com /2007/12/27/ stories/2007122750420200.htm. 196

4. Babbie, Earl. R., & Mouton, J. (2001).The practice of social research. Cape Town: Oxford University Press southern Africa. Balakrishnan.(2009). Cyber Victimization of Women and Cyber Laws in India. Retrieved from http://www.irma-international.org/viewtitle/55537/

5. Barak, A. (2005). Sexual harassment on the Internet. Social Science Computer Review, 23, 77-92.

6. Bowker, A., & Gray, M. (2004).An introduction to the supervision of the cybersex offender. Federal Probation, 68(3), 3-9.

7. Creswell, J.W. (2003). Research design: Qualitative, quantitative and mixed methods approaches. 2nd edn. Lincoln: SAGE. Crime in India (2014).

[67] N.S. Nappinai, Cyber Laws Part II: A guide for victims of cyber crime, Nov 03, 2017, available at: https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms?from=mdr

[68] Dhruti M Kapadia, Cyber Crime Against Women And The Laws In India (2018) **https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/** https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/.

8. Harpreet Singh &Geeta.(2013). Cyber Crime – A Threat to Persons, Property, Government and Societies.International Journal of Advanced Research in Computer Science and Software Engineering.Vol 3(5).Retrieved from http://www.ijarcsse.com/5_May2013.php. 199

9. Davies, P., Francis, P. and Jupp.V. (2011).Doing criminological research.2nd edn. London: SAGE. Dickinson, Julia Phillips. (2006). The phenomenon of cyberstalking on the RIT campus. (Definitions, behaviors and normalization).Thesis.Rochester Institute of Technology.

10. Doring, N. (2000). Feminist views of cybersex: Victimization, liberation, and empowerment. CyberPsychology& Behavior, 3(5), 863-884.

11. E. Ogilvie. (2000). "Cyberstalking," Trends &Isssues in Crime and Criminal Justice, number 166, pp. 1-6. Eurobarometer. (2012).

12. Eytan, A. and Borras, L. (2005) Stalking through SMS: A new tool for an old behaviour?.Australian and New Zealand Journal of Psychiatry 39, 204.

13. Feuer, Bianca S., Psy.D., (2014).The effects of cyberstalking severity, gender, and the victim-perpetrator relationship on reporting to law enforcement. Alliant International University, 2014, 88 pages.

14. Finch (2001). The Criminalisation of Stalking: constructing the problem and evaluating the solution, London: Cavendish.

15. Fisher, B. S., Cullen, F. T., & Turner, M. G. (2000).The sexual victimization of college women. Washington, DC: National Institute of Justice, Bureau of Justice Statistics. Fox, R. (2001). Someone to watch over us: Criminology and Criminal Justice, 1(3), 251-276.

16. Halder, D. (n.d). Cyber crime against women in India". Retrieved from http://www.cyberlawtimes.com/articles/103.html

17. M. R., &Garofalo, J. (1978). Victims of Personal Crime: An empirical foundation for a theory of personal victimization. Cambridge, MA: Ballinger. Holt, T. J., &Bossler, A.M. (2009).Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30, 1- 25.

18. Paullet, Karen L., Rota, Daniel R., & Swan, Thomas T. (2009).Cyberstalking: An exploratory Study of Students at a Mid-Atlantic University. Issues in Information Systems X (2).

19. Reyns, B. W., &Englebrecht, C. M. (2010). The stalking victim's decision to contact the police: A test of Gottfredson and Gottfredson's theory of criminal justice decision making. Journal of Criminal Justice, 38, 998-1005. Retrieved from https://ideas.repec.org/a/eee/jcjust/v38yi5p998-1005.html

20. Reyns, B. W., Henson, B., & Fisher, B. S. (2011).Being pursued online: Applying cyber lifestyle – routine activities theory to cyberstalking victimization. Criminal Justice and Behavior,38(11), 1149-1169. 210

21. Semmens, N. (2011). Methodological approaches to criminological research. In P. Davies, P. Francis, 8: V. jupp (Eds), DoingCriminological Research. London: SAGE Publications, 54-77.

B. Website

1. www.newworldencyclopedia.org/entry/Cybercrime
2. www.bukisa.com/articles/206_internet-security-concepts
3. http://en.wikipedia.org/wiki/Computer_crime
4. http://www.wisegeek.com/what-is-cybercrime.htm
5. http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic_commun_privacy_act.txt
6. http://www.brighthub.com/internet/security-privacy/articles/65042.aspx
7. http://www.securityweek.com/wikileaks-under-denial-service-attack-ddos
8. http://crimesatcyber.blogspot.com/feeds/posts/default?orderby=updated
9. http://news.softpedia.com/news/Internet-Fraud-384.shtml