Available online at www.elixirpublishers.com (Elixir International Journal)

Criminal Law

Elixir Criminal Law 47 (2012) 8891-8895

ISSN: 2229-712X

# Cyber crimes against women in India: Information Technology Act, 2000

Shobhna Jeet
Department of Law in Central University of Haryana, Mahendargarh.

**ARTICLE INFO**

**Article history:**
Received: 3 April 2012;
Received in revised form:
25 May 2012;
Accepted: 12 June 2012;

**Keywords**
Cyber crimes,
Women,
Information technology,
ICT.

**ABSTRACT**
In the digital age, 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 'spying websites' like 'wikileaks'[1] 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.



## Introduction

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[1] 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[2]. 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. 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 cyber socializing communications has remained untouched. The Act turned out to be a half baked law as the operating area of the law stretched Cyber Victimization of Women and Cyber Laws in India. The present study is an attempt to highlight the cyber crimes against women in India. To make the study richer a brief glance of the cyber crime protection laws especially for women in UK and USA is taken as reference point. One might question these reference countries, but there is not much harm to draw some inferences based on their laws. The reason is that the nature of the problems originated from the information and communication technology remain more or less same across the world, however the economic, political and social conditions of these countries is different to each other. Moreover the problem against women such as Harassment via e-mails, Cyber-stalking, Cyber pornography, Defamation, Morphing, Email spoofing, etc. are also treated of the same nature worldwide. The study throws light on the types of cyber crimes against women in India in the light of Information Technology Act, 2000.

## Cybercrime against woman in UK

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 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. 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

[1] The word "Cyber Space" was coined by "William Gibson," the Canadian/American science fiction writer who helped define its cyberpunk sub-genre, in 1982 in his novelette "Burning Chrome" in Omni magazine, and in his novel "Neuromancer".
[2] The Cambridge English Dictionary defines Cybercrimes as crimes committed with the use of computers or relating to computer, especially through Internet.

Tele:
E-mail addresses: shobhna.jeet@gmail.com

offences are imprisonment for a term of 12 months or to a monetary fine not exceeding statutory maximum, or both.

**Protection for Woman against Cybercrime in USA**

USA is one of the countries which evaluated the dark and ugly side of internet; the cybercrimes. A study shows that till 2010 among 349 victims 73 percent are women which evident the vulnerable condition of women in cyberspace. Whereas it recognised 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 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.

**Cybercrime against woman in India**

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. India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes; This Act widely covers the commercial and economic crimes which is clear from the preamble of the IT Act. Most of the cases related to cyber crime 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 following case study.

*Dr.L.Prakash v. Superintendent*[3]

In this case the accused was an orthopedic surgeon forced women to perform sexual acts and later on upload and sale these videos as adult entertainment materials worldwide. He 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 under the Immoral Trafficking (Prevention) Act, 1956.

*State of Tamil Nadu v. Suhas Katti*[4]

In this case the accused Katti posted obscene, defamatory messages about a divorced woman in the yahoo message group and advertised her as a solicit for sex. This case is considered as one of the first cases to be booked under the Information Technology Act, 2000 (IT Act). He was convicted under section 469, 509 of Indian Penal Code (IPC) and 67 of the IT Act 2000 and was punished for 2 years rigorous imprisonment and fine.

Above mentioned cases were considered first time under the ambit of IT Act. Apart from these cases there are few basic cybercrimes that basically happens to the Indian women in the cyberspace such as harassment via e-mail, cyber-stalking, cyber defamation, morphing, email spoofing, hacking, cyber pornography and cyber sexual defamation, cyber flirting and cyber bullying.

**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. 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 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 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. 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 'extra-territorial' jurisdiction. With the advancement of technology that obscene is no longer a local phenomenon. It is now global and dynamic in nature and thus needs strict interpretation of statutes.

**Cyber stalking**

This is one of the most popular about internet crime 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. The University of Virginia defines stalking as behavior wherein an individual

[3] (2008) 3 MLJ (Crl) 578

[4] (2004) also available at www.naavi.org/cl_editorial_04/suhas_katti_case.htm

willfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person. Stalking in the internet happens when the perpetrator follows the victim continuously 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. Most of the cases are reported where the target of cyber stalking are women especially of the age group of 16 to 35.

***Ritu Kohli Case***

Ritu Kohli Case was India's first case of cyber stalking, in this case Mrs. Ritu Kohli complained to police against a person, who was using her identity to chat over the Internet at the website http://www.micro.com/, mostly in Delhi channel for four consecutive days. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu Kohli at add hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on add hours. The said call created a havoc in personal life of the complainant consequently IP addresses was traced and police investigated the entire matter and ultimately arrested the offender. A case was registered under the section 509, of IPC and thereafter he was released on bail. This is first time when a case of cyber stalking was reported.

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**

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. 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 (Section 67 of the IT Act 2000: 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 effect is such as to tend to deprave and to 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 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 one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with a fine which may extend to rupees two lakh. 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".

**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 someone other than the actual sender. Email spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, however this precaution is not always taken.[5] One of the best examples of Cyber spoofing is Gujrat Ambuja's Executive Case[6], in this case the perpetrator pretended to be a girl for cheating and blackmailing the Abu dhabi based NRI.

**Hacking**

Hacking means unauthorized access to computer system or network[7], and it is the most predominant form of cyber crime. It is an invasion into the privacy of data, 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. Even though some social networking communities like Orkut, facebook have the option of reporting profiles as bogus, Photo-Video lock, special tools for reporting, still, many women are kept in dark, when their email IDs or even websites are hacked. There are different classes of Hackers.

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, Section 290 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**

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.

Recently, The Air Force Balbharati School case (Delhi)[8] is a recent case comes under this category where a student of the School was teased by all his classmates for having a

---

[5] http://www.mailsbroadcast.com/e-email.broadcast.faq/46.e-mail.spoofing.htm.

[6] G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology ( 2007)

[7] Section 66 of Information Technology Act, 2000.

[8] Abhimanyu Behera, " Cyber Crimes 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.

In another incident, at Mumbai, a Swiss couple gathered slum children and then forced them to appear for obscene photographs, which they took and then uploaded those photographs to websites specially designed for pedophiles. The Mumbai police arrested the couples for pornography.[9]

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 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).

**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. The accused can be booked under section 67 and 72 of the IT Act as well as IPC as discussed earlier.

**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. Again this can be treated as the flip side of IT Act that 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.

**Cyber bullying**

Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.[10] 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)[11] 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. The story turned to be more terrific when it found that the person was just a creation of some Lori Drew, who was arrested in 2008 for violating the Computer Fraud and Abuse Act but unfortunately was acquitted in 2009.The social network like Orkut, Facebook can be considered the main source of cyber bullying. But despite of the vulnerability of women net surfers IT Act does not provide some direct protection to the victims. While most of the crimes can be booked under IPC, under IT Act there are only three provisions which connote cyber crime i.e. Section 67, 70 and 72. 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 cyber crimes against women under IT Act.

**Reasons for the Growth of Cyber Crime against Women in India**

The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. The study shows that we have 52 million active internet users in India which reached at 71 million in the year 2009. Among them working women net users are 8 percent and 7 percent nonworking women in the year 2009 and 37 percent usage of all users accessing internet through cyber café.[12] It is very common phenomenon that the important information of the net surfer is being disclosed easily by the owners of cyber café and then it is used for illegal purposes. 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 reason for the increasing cyber crime rate against women can be categorized into two folds; legal and sociological reasons.

**Legal Reasons**

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. As we discussed above that majority of cyber crimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form), 72(breach of confidentiality). The most of the cyber crimes other than e- commerce related crime are being dealt with these three sections. Cyber defamation, cyber defemation, email spoofing, cyber sex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions[13]. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 506 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. 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 which covers cyber sex in Toto.

As it has been discussed earlier that transcendental nature of Internet is one of the main reasons for the growth of cyber crime so whereas Section 75 of the IT Act deals with the offences or

[9] G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology ( 2007)

[10] According to Oxford Dictionary

[11] Available at http://blog.koldcast.tv/2011/koldcast-news/8-infamous-cases-of-cyber-bullying/

[12] http://trak.in/tags/business/2010/04/07/internet-usage-india-report-2010/

[13] Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI, *IJCC* 19 (2010)

contravention committed outside India but it is not talking about the jurisdiction of the crimes committed in the cyberspace specially the question of place for reporting the case arises 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.

**Sociological reasons**

Most of the cyber crimes 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 cyber crime 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.

**Conclusion**

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 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.[14] 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.

[14] http://www.genderit.org/es/node/2213)