GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

SCHOOL OF LAW

VICTIMOLOGY

TOPIC:

CYBER CRIMES AND VICTIMISATION OF WOMEN IN INDIA WITH SPECIAL REFERENCE TO CYBER OBSCENITY

SUBMITTED BY:

URVESHI

LL.M (1ST YEAR) (2ND TRIMESTER)

ADMISSION NO.- 20GSOL2010036

SUBMITTED TO:

DR. SHWETA THAKUR

Cyber Crimes and Victimisation of Women in India with Special Reference to Cyber Obscenity

Abstract: **The traditional Indian society places women in a very high regards, the Vedas glorified women as the mother, the creator, one who gives life and worshipped her as a "Devi" or Goddess. The women occupied a vital role and as such her subjugation and mistreatment were looked upon as demeaning to not only the woman but towards the whole society. However, in modern times women are viewed and portrayed as sex objects, she is treated inferior to men in various societal spheres and functions, this has created a huge gender bias between the men and women where even the men think that their wrongdoings towards women cannot be penalised. Cybercrime and internet bullying works in similar manner where the wrong-doers are not afraid of any authority that can penalise. The cyber world in itself has a virtual reality where anyone can hide or even fake his identity, this gift of internet is used by the criminally minded to commit wrongful acts and then hide under the blanket provided by the internet.**

Keywords: **Cyber-Crimes, Cyber Obscenity, Women Victimization, Indecent Representation etc.**

INTRODUCTION

In India, cyber- crime and victimization in the cyber space had remained a subject of great trepidation, but lacks awareness. Bizarre combination of nature of attacks; ever changing trends of the victimization, limited knowledge about direct laws which address cyber-crimes in India and rights of victims in cases of cyber-attacks, contribute greatly towards forming a weird approach to cyber victimization scenario. There are millions of internet users in India now who are frequenting the cyber space on a regular basis for professional, commercial, socializing and educational purposes. Since the IT sector in India have seen a boom in the 1990's, (which still continues), almost every household falling in the economic zone of moderate-income groups to high income groups, have internet access at home and people from the age group of 13 to 70 years, belonging to these clusters, are regularly using the internet either at home, or at work places, or at educational institutes, or at cyber cafes. But along with internet- dependency, victimization of 'cyber citizens' and also of those who are not in the 'internet', have grown in an alarming rate, in spite, India has an exclusive legislation dedicated for information technology, e-governance, e-commerce and also e-socialization to a certain extent; this has hardly helped in curbing the ever-increasing victimization of individuals in the cyber space in India.

Sadly enough, less awareness brings in more victimization and cyber space victimization is no exception. In India, awareness of cyber victimization has remained limited to several informative and useful tips on how to save one's personal computer and personal data from identity- frauds, emotional blackmailers etc.

CYBER CRIME

Cyber-crime is a global phenomenon. With the advent of technology, cyber-crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Even though India is one of the very few countries to enact Information Technology Act[1] to combat cyber-crimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the security of women in general is not covered fully by this Act. Cyber bullying can affect everyone, including children. Safety Web provides support for parents to improve internet safety for kids. Technical measures to protect computer systems are being implemented along with legal measures to prevent and deter criminal behaviour. 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 or network is used as the source, tool or target is known Cybercrime.[2]

CYBER CRIME AGAINST WOMEN

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. Safety of women has always been an issue, especially in a country like India where worm of crime rate against women is increasing like a coconut tree. Earlier, it was limited to roads or at places away from Home. Home was the safest place for a woman to protect herself from being victimized, but not now. Home is becoming equally dangerous place, prone to crime for them. The limit is set to their computer screens, however. This is a major concern. The increasing rate of cyber-crime against women has led to development of insecurity within a woman. They don't feel safe anymore, anywhere. Its effects are worse on them and on the society as a whole, when we look into the broader picture.[3]

"A subcategory of computer crime and it refers to criminal offenses committed using the internet or another computer network as a component of the crime." -Shinde

[1] 2000

[2] Desai, M. and Jaishankar, K (2007), Cyber Stalking-Victimization of Girl Student: An Empirical Study

[3] "Cyber-crimes against women in India: IT Act, 2000"

TYPES OF CYBER-CRIMES AGAINST WOMEN

In basic terms, cyber-crime is any illegal activity that uses a computer as its primary means of commission. It is expanded to include actions like a criminal offense on the web, a criminal offense regarding the Internet, a violation of law on the Internet, an illegal activity committed through Internet, breach of law on the Internet, computer crime, contravention of any law through the Web, corruption regarding Internet, criminal activity on the Internet, disrupting operations through malevolent programs on the Internet, electric crime, Internet crime, sale of contraband on the Internet, stalking victims on the Internet, theft of identify on the Internet. Cyber-crimes may be committed against persons, property and government. The common types of cyber-crimes are discussed below.

- **Harassment through e-mails:** It is not a new concept. It is very similar to harassing through letters. It includes blackmailing, threatening, bullying, and even cheating via email. Though E-harassments are similar to the letter harassment but creates problem quite often when posted from fake ids.

- **Cyber stalking:** It is one of the most talked about and committed net crimes in the modern world. Stalking is defined as pursuing stealthily according to the Oxford dictionary. Following a person's movements across the Internet by posting messages sometimes threatening on the bulletin boards accessed by the victim, entering the chatrooms used by the victim and by constantly bombarding the victim with emails, messages etc. constitutes a cyber stalking.

Ritu Kohli Case

Ritu Kohli Case[4] 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.

- **Cyber pornography:** It is the most dangerous threat to the female netizens. This would include pornographic websites or pornographic magazines produced using computers to publish and print the material and the Internet (to download and transmit pornographic pictures, photos, writings etc. Internet has provided a medium for the facilitation of crimes like pornography, especially cyber porn. Today, almost 50% of the web sites contain pornographic material on the Internet. This turns dangerous to a woman's integrity as cyber criminals use photos of women and fix them with nude Photographs or videos and the photograph or video resembles of that woman only.[5]

---

[4] 2001, http://cyberlaws.net/cyberindia/2CYBER27.htm

[5] Haider, D., & Jaishankar K. (June 2011) Cyber-crime and the Victimization of women

The DPS MMS scandal[6] is a very famous case of this where an MMS clip of a school girl in compromising situation was made and distributed amongst various internet networks.

The most recent example is of **Delhi Metro CCTV footage leaks case**,[7] where the CCTV recording couples getting intimate in metro stations etc. which has been recorded by police security cameras has been leaked on internet.

- **Cyber defamation:** Cyber tort including libel and defamation is another common crime against women on the net. This occurs when defamation takes place with the help of computers and/or the Internet. For example, someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends or relatives. It is mostly committed by hacking someone's id. on Facebook, Google, or any other social networking or mailing website. It is also done by creating fake profile of a person containing all personal information about that person, which resembles to be a genuine one to others on any website.

The very first instance of cyber defamation in India was recorded in the case of **SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra**[8] - cyber defamation was reported when a company's employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Another famous case involving a woman was **The State of Tamil Nadu Vs Suhas Katti**[9] **-** The case is related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

- **Morphing:** Editing of the original picture by unauthorized user or fake identity is termed as Morphing. It was identified that female's pictures are downloaded by fake users and again re-posted/uploaded on different websites by creating fake profiles after editing it.

Air Force Bal Bharati School case (Delhi)[10] comes under this category where a student of the school was teased by all his classmates for having a pockmarked face. He, who is tired of the cruel jokes, decided to get back at his tormentors and scanned photograph of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. The father of one of the class girls featured on the website came to know about this and lodged a complaint with the police. Such acts can be

---

[6] http://en.wikipedia.org/wiki/DPS_MMS_Scandal
[7] https://zeenews.india.com/nation/porn-mmses-from-delhi-metro-cctv-footage_860933.html
[8] http://cyberlaws.net/cyberindia/defamation.htm
[9] http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm
[10] Abhimanyu Behera, "Cyber Crimes and Law in India."

penalised under I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC sec 509 also.

- **Email spoofing:** An e-mail which misrepresents its origin is a spoofed mail. It shows its origin to be different from which actually origin.[11]

The most popular case of cyber spoofing is **Gujrat Ambuja's Executive Case,**[12] in this case the perpetrator pretended to be a girl for cheating and blackmailing the Abu Dhabi based NRI.

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. Studies 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% and 7% nonworking women in the year 2009 and 37% usage of all users accessing internet through cyber cafe.[13] It is very common occurrence that the essential data of the internet surfer is being released effortlessly by the owners of cyber cafe and then it is used for illegitimate dedications. Though acquaintance with technology is constructive facet that can be considered vital for the progress of any country but at the same time it is becoming the foundation to upsurge the offense rate with technology against the weaker sector of the society.

The reasons for the growth of cybercrime rate against women can be categorized into two folds:

(1) Legal Reasons

The objective of the IT Act is crystal clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e., hacking, fraud, and breach of confidentiality etc. but the drafters were unacquainted with the protection of net users. As we deliberated above that majority of cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form), 72(breach of confidentiality). The most of the cybercrimes other than ecommerce related crime are being dealt with these three sections. Cyber defamation, cyber defamation, email spoofing, cybersex, 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.[14] Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 509 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, however until recently there were no specific penal provisions protecting women specifically against internet crimes. Ever since the 2012 Delhi Gang Rape case (Nirbhaya Case) there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the criminally minded. The 2013 Criminal Law Amendment Ordinance contains several additions to the Indian Penal Code, such as to

[11] "Indian Women at Risk in the Cyber Space"
[12] http://www.indiaforensic.com/cyberextortion.htm
[13] http://www.acadmia.edu/440672/Cyber_Victimization_in _India_A_baseline_survey_report_2010
[14] Abhimanyu Behera, "Cyber-crimes and Law in India"

sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner.

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

(2) Sociological reasons

Most of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times, she considers that she herself is accountable for the crime done to her. The women are more vulnerable 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. Women fear that reporting the crime might make their family life difficult for them, they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher.

IMPACT OF CYBER-CRIME

Under this technological development era the most effected victim is women. Every sphere of life now a day, start and end with digital intervention i.e., computer technological interferences. In the light of this, the positive as well as negative sides also come out. Cybercrime is a global phenomenon. The advancement of technology, cybercrime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. The privacy and personal security of the individual are under threat with this growing issue of cybercrime in the cyberspace.[15] Internet is world's largest information system and giant network. As telecom infrastructure developments continue to penetrate into smaller towns, Internet usage numbers showcase the effects with its ever-increasing base of users. The Internet is now a part of the globalization process that is evidently sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a compact world. The cyberspace has been a blessing to human civilization. Internet has connected people around the globe. The desire to know what is unknown is indispensable of human nature. It is the desire to know about the people, who inhabit the earth, has aggravated the urge of discovering the untraded path. This has led to the unearthing of the cyber world.

[15] https://www.legalserviceindia.com/artic les/etes.htm

CYBER OBSCENITY

Indian View on Obscenity-

- Whichever work with the intention of appealing to prurient interest
- Whichever work, highlights sexual behaviour in a blatantly unpleasant manner.

In legal terms obscenity can be described as a licentious phrase, such as words, images, and actions, exhibiting acts which are indecent and that leads to immoral influences of one's imagination, is a breach of the Indian Law. The Indian Constitution evidently sets out limitations on freedom of speech guaranteed under article 19(1) (a) can be subject to limitation to maintain decorum or principles. It can be coined as "repulsive to decorum". If the publication as a whole, implicates to distort the mind of people who are exposed to such influence, is termed obscene. The literal or dictionary meaning for it is, "words, thoughts, books picture etc. morally disgusting, offensive". Alpana Poddar, a SC lawyer says "does not have any clear-cut definition on this. It depends on facts of the case". Former Member of the parliament and lawyer RK Anand adds on to it by saying that obscenity can be a wide word as, what was considered as obscene 20 years before, may not be considered obscene now.

Section 292 of the Indian Penal Code deals with obscenity offences in India, the section counters one's right to freedom of expression, which assured by the constitution of India, but Article 19(2) of the constitution provides that right to freedom of expression is open to limitations for prevention of indecency in public interest. Section 292 of Indian Penal Code provides that sale of books, pamphlets, paper, writing, drawing, painting, representation, figure or any other object shall be deemed obscene if it is licentious or pleads to the prurient concern or if its outcome, if the major part tends to degrade a person, who are likely to get exposed to it.

A penalty of two years along with a fine up to rupees two thousand (Rs.2000) is prescribed under the Indian law for an individual who advertises obscenity, such as sells, possess, hire, imports, makes profit from such business, if he is found accountable for the succeeding time, captivity for up to five years and a fine up to rupees five thousand (Rs.5000) is served as retribution.

In **Ranjit D. Udeshi vs. State of Maharashtra,**[16] the court said that the check of obscenity in India is whether obscenity is available with a profitable or marketable purpose and no other societal intention. It shouldn't have the constitutional defence of freedom of speech. In case of relation of art with obscenity the court said that 'the art must be so preponderating as throw obscenity into a shadow or the obscenity so trivial that it can have no consequence and can be ignored'.

Cyber obscenity

The internet began in 1969 as a project of APANET a branch of the department of defence[17]. Internet today is the easiest and admired way of interaction because it is simple and user-friendly. Everybody has the right to use the internet and view, share, download any document

[16] 1965 AIR 881, 1965 SCR (1) 65

[17] Maureen A. O'Rourke, Fencing Cyberspace: Drawing borders in Visual World, 82

or file from the website that he/she finds on the internet[18]. But some the websites contain sexually explicit materials which are harmful for children, the principal concern of parents lies on the fact that the easy access to such pictures by just "pointing and clicking" is a simple task for a small child. Also, a woman in relationship, naturally will not inquire the intention of her spouse and permits to capture moments of their physical relationship. Women who are photographed either casually or in exposed situations by strangers who blackmail them later or use these to lure them into their "adult industry". Apart from these men have been editing pictures of women who either dump them or abandon them. The internet is the safest avenue for distribution of pornography as the distributor and receiver remains anonymous.

In the United States the Communications Decency Act 1996 (Title V of the Tele communications Act 1996) was an attempt to make Internet "superhighway safe place for our children and our families to travel on"[19] . The solitary purpose of CDA was to guard the minor from any obscene, lewd, filthy content on the internet. Also, the CDA made it an unlawful offense to use computer to communicate with minor and transmit the described sexual or excretory activities, or to communicate in a manner that is easily available by anybody under the age of eighteen. In Reno vs. ACLU[20], the Supreme Court of U.S invalidated the CDA indecency provision of 47 U.S.C 223(a) and 223(d) in 7-2 decision. The government argued that it was constitutional as it was to defend and preserve the interest of the minor, but the court said that although the safety of children from sexually explicit content had been governments compelling interest, but the CDA provisions censored an intolerable amount of legally secured dialogue for adults. Possession of obscene material with the intention to distribute or to receive from a carrier in interstate or foreign commerce is a crime.

In India, Information Technology Act, 2000 contains the term cyber obscenity. According to this Act storing or individual (private) viewing of obscene material is legal as it does not specifically restrict it, but transmission and distribution of such is illegal. Section 67 was the only provision of the IT Act that prohibited release of obscene material till 2008. Section 67(A) deals with restriction in publication of any content that is sexually explicit and Section 67(B) prohibits publication of child pornography. This section makes transmission and distribution of such material a criminal offense but downloading, storing or viewing of such is not an offense under this law. The essentials of this section are (i) the transmission should be made in electronic form (ii) It should appeal to prurient interest. The penalty under this section is any person who is declared guilty, should be imprisoned for up to three years or as decided by the court with a fine of rupees five lakhs (Rs. 500000) in First conviction, and if he is declared responsible for the succeeding time, captivity up to five years and a compensation of rupees ten lakhs is served as punishment. The penalties for these offenses include fines, imprisonment for up to two years, or both.

[18] Reno I. 929 F, Supp. At 836-37
[19] 141 CONG REC. S8087-04 (JUNE 9,1995)
[20] 117 S Ct. 2329 (1997)

LAW PERTAINING TO ELECTRONIC MEDIA AND CYBER OBSCENITY

Cyber laws 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.

- Section 65, Chapter XI of the IT Act deals with the offences such as Tampering with computer source documents (s.65).
- Section 66 Hacking with computer system (s. 66)
- Section 67 publishing of information which is obscene in electronic form (s.67).
- Section 70 Access to protected system (s. 70)
- Section 72 Breach of confidentiality and privacy (s. 72)
- Section 74 Publication for fraudulent purpose (s.74) IT Act 2000 still needs to be modified.
- 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.[21]

IT Act, 2008

- 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.[22]

IPC, 1860

- Section 292 deals with sale, etc., or obscene books, etc
- Section 293 deals with sale, etc., of obscene object to young person
- Section 294 deals with obscene act and songs

"A crime related to technology, computers, and the Internet." -Schell & Martin

[21] IT Act, 2000
[22] IT Act (Amendment) 2008 Section 67(A)(B)(C).

INDECENT REPRESENTATION OF WOMEN (PROHIBITION) ACT

As has been stated above, Indecent Representation of Women (Prohibition) Act was created to address representation of women which may not fall under the purview of 'obscenity'. The law was created to prohibit indecent representation through publication which can be communicated to any individual or general public through two main channels: (i) advertisements and (ii) physically sending any book, pamphlets, paper, slide, film, writing, drawing, painting, photograph, representation or figure which contains indecent representation of women. The term 'indecent representation of women' was defined as "depiction in any manner of the figure of a woman; her form or body or any part thereof in such way as to have the effect of being indecent, or derogatory to, or denigrating women, or is likely to deprave, corrupt or injure the public morality or morals".

CASE STUDY

In the case of **Awnish Bajaj v. State (NCT) of Delhi**[23] popularly known as DPS MMS Scandal, an MMS where a DPS girl was involved in a highly sexually explicit act was uploaded on a website named "baazee.com" for sale and several copies of the MMS were sold making a huge amount of profit. The CEO, Avnish Bajaj of the website company was charged under Section 67 of IT Act for publication and transmission of obscene materials but the defendant argued that he was not directly involved in the case and since the Section prohibited publication and transmission of obscene materials, his act did not amount to any of such activities and the company took all reasonable steps to remove the video after 38 hours and the delay of 38 hours was due to the intervention of the weekend. His arguments were agreed by the landmark court and he was enlarged on bail.

In the case of **Syed Asifuddin v. The State of Andhra Pradesh,**[24] Tata Indicom interfered with a scheme of Reliance Info COMM where Reliance introduced a mobile handset in the market at a reasonable price but the services under the scheme were restricted only to Reliance Info COMM. The employees of Tata indicom somehow managed to manipulate the mobile handset and started providing their own services which caused a loss to the Reliance Company. Later when the matter was brought before the court, Tata Indicom employees argued that they committed no offence under IT Act. But the court refused their arguments and held that the mobile phone comes within the meaning of the term 'Computer' under Section 2 of the Act and thus their act constitutes an offence under Section 65.

In the case of **PR Transport Agency v. Union of India,**[25] a contract reached through email between two parties was the issue where the defendant first entered into a contract and later rescinded it on an excuse of technological grounds. The defendant argued that the court did not

[23] (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427, 2005 (79) DRJ 576.
[24] 2006 (1) ALD Cri 96, 2005 CrimLJ 4314.
[25] AIR 2006 All 23, 2006 (1) AWC 504.

competent jurisdiction to try the case, since the place of receiving the email was outside the territorial jurisdiction of the concerned court. The court rejecting the defendant's argument interpreted Section 13 of the IT Act which lays down the general provision regarding contract reached through email. It says that in cases of contract by emails, the usual place of occurrence of the business shall be taken into consideration for determining the jurisdiction of a particular court when any dispute arises, since emails can be received at any place in the world therefore taking into consideration the place of receiving the emails will amount to a lot of practical hardships.

In the case of **Times Internet v. M/s Belize Domain Who is Service Ltd,**[26] the plaintiff was running a website named 'indiatimes.com' and provided a number of services including travel services, while the defendant registered a domain name 'indiatimestravel'.com' and started offering travelling services in the domain name 'travel.indiatimes.com'. when the dispute between the two was brought before Delhi High Court, it was held that the act of defendant constituted the offence of cyber-squatting that is similar to passing off in case of trademarks since both the domain names were deceptively similar. The court followed the judgment that was laid down in the case of Satyam Info way Limited v. Sifynet Solutions Pvt Ltd.

In the case of **NASSCOM v. Ajay Sood,**[27] the court went on to set a precedent as regards the offence of phishing by holding that any act of misrepresentation in the usual course trade that causes confusion as regards the origin and the source of email which results into grave loss of the customer as well as the person whose name and identity were used will lead to phishing. In this case the defendant collected personal information from different individuals in the name of the plaintiff through emails. Later the court held the defendant guilty for committing the offence of phishing and made the defendant to pay compensation to the plaintiff. By this case only phishing was brought within the scope of India laws which means that IT laws are incomplete and cannot be held to be exhaustive in its own sphere since much of its scope were clarified through judicial interpretations.

RECOMMENDATION

- Don't be a liability on the society, always be an asse, and before thinking about committing any offence, think about its consequences.

- "Prevention is better than cure". So, all the net users, especially women, who are more prone to be the victims of cyber-crime, should not share their personal information to public.[28]

- Social Networking sites like Face book, they should maintain the privacy limit on their information and photos.

- They should be careful in adding strangers in their friend list.

---

[26] CS(OS) No. 1289/2008.
[27] 119 (2005) DLT 596, 2005 (30) PTC 437 Del.
[28] http://delhicourts.nic.in/ejournals/CYBER%20LAW.pd.

- The less accessible their private information and photos will be, the safer they are, behind the screens.

- If any cyber-crime happens against them, they should immediately report it to the cyber cell of police and ask for immediate actions.

- Vishakha Singh, they should teach a good lesson to each abuser and defamer. Despite sitting and suffering silently, they should fight for their justice, because "If you do not offend the crime, crime will offend you".[29]

- Indian Legal system, as well as Indian justice delivery system is that effective laws should be enacted through required amendments in the present statutes, that can tackle such issues of cyber-crime against women and can provide for deserved punishments to the offenders.

- Internet security is of vital importance and needs to be taken care of. Also, justice delivery should be speedy and effective.

- Present law should not lead to injustice being delivered.

- To prevent and stop crime, some strict actions need to be taken.

- Those actions should be immediate and effective.

- There is no benefit of delay, because "Justice delayed is justice denied."

CONCLUSION

Cybercrimes against women are still taken lightly in India, mostly because in general the respect towards women in our modern society is on a decrease also a lot of people are unable to come to terms with the fact that even posting images of someone online in a crime. Cybercrimes such as morphing, e-mail spoofing do-not have a moral backing in society and hence are taken lightly. This brings us to the most important part where social advancement is needed, people need to recognise the rights of others and realise what constitutes a crime.

They must learn not to interfere with the private lives of others, respect towards women in society needs to increase. All this can only be done if young kids are taught from a young age to respect women.

Hence, to counter cybercrime against women in India, not only stricter penal reforms are needed but also a change in education system is a huge requirement. Such change cannot come from within a single block of society but people, government and NGOs etc. need to work together to bring forth such changes.

REFERENCES

- Halder D., & Jaishankar, K. (2008) Cyber-crimes against women in India.

[29] Vishakha and Ors. Vs. State of Rajasthan and Ors. (JT 1997 (7) SC.

- Halder D., & Jaishankar, Cyber Victimization in India: A Baseline Survey Report.
- Verma, A. (2009) Cyber-crimes and Law. India: Central Law Publishers.
- Information Technology Act, 2000.
- Information Technology Act, 2008.
- Desai, M. and Jaishankar, K (2007), Cyber Stalking-Victimization of Girl Student: An Empirical Study.
- http://delhicourts.nic.in/ejournals/CYBER%20LAW.pd.
- http://www.acadmia.edu/440672/Cyber_Victimization_in_India_A_baseline_survey_report_2010.