

VICTIMIZATION OF WOMEN BENEATH CYBERSPACE IN INDIAN UPBRINGING

Dr. Monika Jain*

"Cybercrime as crime committed over the Internet."

-The Oxford ReferenceOnline

Abstract

This research study provides a review and analysis of the development of regulatory instruments statutes, recommendations, guidelines, etc. to protect privacy and related interests of women in cyberspace. These instruments form a field of law and policy that has attained considerable maturity, spread and normative importance over the decades. The awareness of the individuals regarding the law and policy in this concern is the prime objective and which will reflect the status of India. All-encompassing the regulatory field is an immense body of academic commentary analyzing privacy issues in cyberspace from a variety of perspectives. This paper presents a predictive analysis of cyber-crimes against women in India and laws that prevent cyber victimization in general and women in especially. Cyber-crime is broadly used to describe the activities in which computers or networks are a tool, a target, or a place for criminal activity. Advancement in technology has led to a steep increase in cyber-crimes and victimization of women in the cyber world. India is among the very few countries to enact Information Technology (IT) Act 2000 to curb cyber-crimes. The world of internet provides every user all the required information fastest communication and sharing tool making it the most valuable source of information. With the numerous advancement of internet, the crime using internet has also widened its roots in all directions. The cyber-crimes pose a great threat to individuals. Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. In this paper we explore the cyber-crimes and the online security vulnerabilities against women. Cyber-crime is emerging as a challenge for national and economic security.

Keywords: cyber-crime, India, women, IT Act 2000, technology

* Dr. Monika Jain, Senior Advocate, High Court of Delhi, Delhi.

Introduction

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 IT Act 2000 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 behavior. But this technology knows no physical boundaries; it flows more easily around the world subsequently the criminals are increasingly located in places other than where their acts produce their effects and Cyberspace is no exception to it. Cyberspace is a new horizon controlled by machine for information and any criminal activity where computer or network is used as the source, tool or target is known Cybercrime.¹ 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

¹ Desai, M. and Jaishankar, K (2007). Cyber Stalking-Victimization of Girl Students: An Empirical Study.

safe anymore, anywhere. Its effects are worse on them and on the society as a whole, when we look into the broader picture.²

"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."

-Schinder

Objectives of this study

- To analyze crime against woman through cyber laws.
- How to compare the equality between the man and women.
- Cyberspace limits for protect for women anywhere.
- Insecurity of woman increase cyber-crime.
- To examine the all laws whether traditional or modern technology act, means.

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

² Shobhna Jeet, "Cyber-crimes against women in India: Information Technology Act, 2000" Elixir Criminal Law 47 (2012) 8891-8895, Elixir International Journal.

Internet by posting messages sometimes threatening on the bulletin boards accessed by the victim, entering the chat-rooms used by the victim and by constantly bombarding the victim with emails, messages etc. constitutes a cyber stalking.

- **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.³
- **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 *Face Book*, *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.
- **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.
- **Email spoofing:** An e-mail which misrepresents its origin is a spoofed mail. It shows its origin to be different from which actually origin.⁴

³ Halder, D., & Jaishankar K. (June, 2011) *Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global. ISBN: 978-1-60960- 830-9.

⁴ Tanaya Saha, Akancha Srivastava, "Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization", *International Journal of Cyber Criminology* Vol 8 Issue 1 January - June 2014.

"Cyber-crime is as any activity that uses the internet to commit a crime."

-Milhorn

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.⁵ 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.⁶

- The social networking websites have developed a new arena for socializing.
- Irrespective of any distinction, women in the society are exulting with this liberation to the fullest.
- From online shopping to net banking, from e-ticketing to e-tax filling, it has made the life of Indian women easy
- It has enabled women to fight for equality even within the confines of their society.
- They can now share their experiences to the whole world,
- To voice their struggles and success in life, it inscribes new spaces of power, which is accompanied with knowledge.

⁵ <http://www.legalserviceindia.com/articles/etea.htm>.

⁶ Fabio Marturana, Simone Tacconi and Giuseppe F. Italiano (2013). Cybercrime and Cloud Forensics: Applications for Investigation Processes (pp. 313-330).

- The internet is serving as boon, but on the other side, it has made the life of women insecure due to rising cybercrime in the virtual world.
- Women of all ages and milieu are in jeopardy with the coming up of internet
- While many women are victimized online, what makes Indian women unique?
- India is predominantly patriarchal and orthodox country and women who are victimized are mostly blamed and online victims are no exception
- Penetration of Information and Communication technologies offers great opportunities and more and more users are getting connected.
- The cost of owning Internet enabled devices has also facilitated to this growth.
- The increase in penetration of ICT, has spurred a growth in ICT-based businesses and services.
- The ICT sector with its direct and indirect contribution to various socioeconomic parameters.
- global player as provider of world class ITES enabled solution and services,
- Various parameters like employment, standard of living and diversity among others.
- IT-enabled initiatives like Government to citizen services, public distribution systems, Healthcare, e-Learning and mobile banking, etc.⁷

“Computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks”.

-Thomas & Loader

Traditional laws for female stratum

The difference between a man and a woman has certainly taken a form of a monster which is now feeding on the female strata of society. There would be no women in India if we do not act now.

Indian Penal Code, 1860

- Section 354 Assault or criminal force to woman with intent to outrage her modesty.
- Section 354 (A), (B), (C), (D)

⁷ Sarabjot Singh Anand, Arshad Jhumka and Kimberley Wade (2011). International Journal of Digital Crime and Forensics (pp. 16-34).

- Section 359-Kidnapping, Section 360 and Section 361
- Section 509-Eve Teasing (Sec. 509)
- Section 378-Chain snatching (Sec 378)
- Sections (376,376A,376B,376C,376D)-Rape
- Domestic Violence-(Sec. 498A)
- Section 506 part II of the section which prescribes punishment for criminal intimidation to cause death or grievous hurt
- Section 120-B-criminal conspiracy
- Section 441 of the IPC-criminal trespass
- Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail
- Honor Killing
- Dowry deaths
- Sections (Sec. 326A, 326B)-Acid attacks
- Section (Sec. 354D)-Stalking
- Sections (Sec. 370, 370A, 372, 373)-Women trafficking⁸
- Sexual Harassment of Women at Workplace Act, 2013⁹
- Protection of Children Against Sexual Offences Act, 2013¹⁰

Cyber laws in India

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.

- 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)

⁸ Indian Penal Code, 1860.

⁹ Sexual Harassment of Women at Workplace Act, 2013.

¹⁰ Protection of Children Against Sexual Offences Act, 2013.

- 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, 1956.¹¹

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.¹²

"A crime related to technology, computers, and the Internet."

-Schell & Martin

Position of Indian law

In India, the Information Technology Act was passed which gave a legal recognition for all transactions and activities carried out by means of electronic communication. The Act deals with the law relating to Digital Contracts, Digital Property, and Digital Rights. Any violation of these laws constitutes a crime. The Act provides for very high punishments for such crimes. The Information Technology (amendment) Act, 2008 (Act 10 of 2009) has further enhanced the punishments. Life imprisonment and fine up to rupees ten lakhs may be given for certain classes of cyber-crimes. Compensation up to rupees five crores can be given to affected persons if damage is done to the computer, computer system or computer network by the introduction of virus, denial of services etc. Even though India is one of the very few countries that enacted IT Act to combat cyber-crimes, but issues regarding women are still untouched in this Act. As it is clear from the preamble of the act, it widely covers economic and commercial issues.¹³

¹¹ IT Act, 2000.

¹² IT Act (Amendment) 2008 Section 67(A)(B)(C).

¹³ The Information Technology Act 2008, Ministry of Law, Justice and Company Affairs (Legislative Department).

Manish Kathuria was arrested by the New Delhi Police. He was stalking an Indian lady, MsRituKohli by illegally chatting on the Web site MIRC using her name, used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, Ritu kept getting obscene calls from everywhere, and people promptly talked dirty with her.¹⁴

Dr. L. Prakash v. Superintendent: 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, 367 and 120-B of the IPC and Section 67 of Information Technology Act, 2000. He was sentenced for life imprisonment and a pecuniary fine of Rupees 1, 25,000 under the Immoral Trafficking (Prevention) Act, 1956.¹⁵

State of Tamil Nadu v. SuhasKatti: 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 imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.¹⁶

- Cyber-crime against women is an issue of which a few talk about and little work on and which is suffered by huge numbers of victims helplessly.
- India is mostly used to cover sexual crimes and sexual abuses in the internet, such as morphing the picture and using it for purposes of pornography, harassing women with blackmailing mails or cyber stalking.
- Nature of sexual crimes.
- Eve teasing.¹⁷

Wrapping up

Cyber abuse or the cyber-crime goes unreported as Indian women are unaware of such offences. While people do not live in cyber space, they come and go like any other place. This nature provides the offenders the chance to escape after the commission of cyber-

¹⁴ <http://www.legalindia.in/cyber-stalking-the-impact-of-its-legislative-provisions-in-india>.

¹⁵ *Dr. L. Prakash v. Superintendent* (Madras High Court, W.P. 7313, 2002).

¹⁶ *Tamil Nadu v. SuhasKutt*, 4680 of 2004 Criminal Complaint.

¹⁷ Jaemin Park (2012). Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 341-362).

crime. The biggest problem of the cyber-crime lies in the *modus operandi* and the motive of the cyber-criminal. Many websites and blogs provide security tips for the safety of women and children while using internet. But still the cyber-crime against women is on the rise.¹⁸ IT Act 2000 defines some cyber-crimes and their punishments but all these are mostly dealing with the economic and financial issues.

- Issues directly affecting the women and the children are nowhere discussed in the act.
- Typical cyber-crimes against women like cyber stalking, morphing and email spoofing are not considered as offences in the act.
- These are the issues affecting the women at large and when they are not protected or prevented by the statute, this loophole encourages the cyber criminals or stalkers to pursue with these shameful activities.
- To reduce and prevent cyber-crime against women, or to be precise, to protect their modesty being outraged through the means of internet, the Indian legal system needs to come up with some amendments in the present statutes, both in IT Act, as well as IPC, to define and punish for such activities affecting the women at large.
- It is the right, as well as the duty of victims of cyber-crime, or of any kind of crime, to report it so that necessary actions can be taken, offenders can be punished, and further crime rate can be decreased.
- Victims are silent, bear all embarrassments, and thus, punish them only for the crime which is done against them.¹⁹
- They do not realize that offender deserves that punishment, not the victims.
- There are always a fear in their minds of being a source of fun and embracement in the society which prevents them to ask for their justice.
- Crime not being reported, and unfortunately gives rise to the crime rate, as the fear of being caught or punished vanishes from the minds of offenders.

¹⁸ Giorgio Calandriello and Antonio Liroy (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 571-586).

¹⁹ Bernadette H. Schell and June Melnychuk (2011). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 144- 169).

Recommendations

- 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.²⁰
- 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.
- The less accessible their private information and photos will be, the more safe 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"*.²¹
- 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."*



²⁰ <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>.

²¹ *Vishaka and Ors v. State of Rajasthan and Ors.*(JT 1997 (7) SC.