Chapter 4.3
Cyber Victimization of Women and Cyber Laws in India

Debarati Halder
Centre for Cyber Victim Counselling, India

K. Jaishankar
Manonmaniam Sundaranar University, India

CHAPTER OVERVIEW

This chapter provides a situational analysis of cyber crimes against women in India and laws that prevent cyber victimization in general and women in particular. The Chapter is divided in to three parts. The part one provides a Situational analysis of cyber victimization of women in India where a pilot study on cyber victimization is also discussed. The Part two of this chapter deals with the current legal protection that are available to women victims in India for cyber crimes such as Offensive communication, Offences against cyber privacy, hacking, stalking and related crimes, Cheating by impersonation, Voyeurism, Pornography, obscenity and indecent representation of women in the cyber space. The part three discusses on various loopholes that exist in Indian laws especially the Indian Information Technology Act and suitable solutions are provided.

INTRODUCTION

In India, cyber crime against women is relatively a new concept. It can be noted that when India started her journey in the field of Information Technology, the immediate need that was felt is to protect the electronic commerce and related communications and not cyber socializing communications. The drafters of the Indian Information Technology Act, 2000, created it on the influence of the Model Law on Electronic Commerce, which was adopted by the resolution of the General Assembly of the United Nations in 1997. The Act turned out to be a half baked law as the operating area of the law stretched beyond electronic commerce to cover cyber attacks of non-commercial nature on individuals as well. While commercial crimes and economic crimes

DOI: 10.4018/978-1-61350-323-2.ch4.3

were moderately managed by this Act, it miserably failed to prevent the growth of cyber crime against individuals including women (Halder & Jaishankar, 2008). However, it took nearly eight years for the Indian parliament to create a modified all exclusive information technology law which tries to regulate illegal cyber activities with prime focus towards protection of electronic commerce. During this gap of eight years of the chaotic lawless situation, 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 hugely discouraged to report the crimes by peers; immediate media attention and the attitude of confused government reporting agencies made women victims more traumatized than they were due to cyber crime meted out to them.

PART I: SITUATIONAL ANALYSIS OF CYBER VICTIMIZATION OF WOMEN

The 'Gestation Period'

In India, 'cyber crime against women' was an issue of which few talked about and few worked on and which was suffered by huge numbers of victims helplessly. The term 'cyber crime against women' in 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 sexually blackmailing / harassing mails or messages etc, or cyber stalking (Balakrishnan, 2009; Mohan, 2004). 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. The following examples depict the situation on this issue:

In the case of 'Sex Doctor', the accused an orthopedic surgeon named Dr. Prakash was found guilty 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). Dr. Prakash was accused of taking obscene pictures and videos by forcing women to perform sexual acts and then later uploading and selling these videos as adult entertainment materials abroad. He was sentenced for life imprisonment and a pecuniary fine of Rupees. 1,25,000 under the Immoral Trafficking (Prevention) Act (CNN-IBN, 2008).

In the case of *State of Tamil Nadu vs. Suhas Katti*, which is considered as one of the first cases to be booked under the Information Technology Act, 2000 (IT Act); the accused Katti posted obscene, defamatory messages about a divorced women in the Yahoo message group. The accused advertised the victim as one who solicits for sex. The accused was convicted under sections 469, 509 of Indian Penal Code (IPC) and 67 of IT Act 2000 and was sentenced to undergo 2 years rigorous imprisonment and fine (India News, 2010).

The above-mentioned cases were the first of its kind that were reported in India after the IT Act 2000 came into existence. Halder and Jaishankar (2008) have explored ten basic types of cyber crimes that happen to Indian women in the cyber space. These are: Harassment via e-mail, Cyberstalking, Cyber defamation, Hacking, Morphing, Email spoofing, Cyber pornography, Cyber sexual defamation, Cyber flirting and Cyber bullying. However, the Indian criminal justice machineries, media and the victims limit their outlook only to sexual crimes, harassing mails and stalking and the awareness of other crimes targeting Indian women in the cyber space remain limited. The rate of reporting of the crimes was low as the present legal infrastructure often failed to mete