Chapter 7
Cyber Space Regulations for Protecting Women in UK

CHAPTER OVERVIEW

This chapter describes various features of regulation of cyber space by the UK. The regulations for unauthorized access and related activities, stalking and stalking related activities, gender sensitive offensive communications and sexual offences are discussed in detail. The issue of consented and unconsented sexual exposure in the internet and various regulatory provisions related to that is also analyzed. A discussion is followed, where an emphasis is made for creation of new women centric laws for their protection in cyber space, as the current laws which are dealing with crimes against women in the cyber space, are found to be archaic.

7.1 INTRODUCTION

Recognition of gender sensitive cyber crimes as a potential danger to the society began in UK only in the late 90's with wide spread discussions in the news media about stalking female celebrities through internet (Ellison & Akdeniz, 1998). In practice, cyber crime research scenario in the UK is more oriented towards analysis including drafting of legislations, for cyber crimes targeting national safety, financial security, corporate identities and information and child safety. Cyber harassments and offences against women are comprehensively covered by the Protection of Harassment Act, 1997. When compared with the US, the UK scenario is more conservative to regulate gender centric cyber harassments except those which involve physical harm.

DOI: 10.4018/978-1-60960-830-9.ch007

This is more evident from the available statistical reports of cyber crime in the UK. Analyzing the 2008-2009 report of "Garlik", "The online experts",[1] it can be seen that among 29.7 million adult internet users in UK, there are approximately 2,374,000 instances of online harassment.[2] By online harassment, the report indicates cases of mental distress of the victim, stalking, sending unwanted abusive mails containing hate messages, racial messages, threatening messages and blackmailing mails etc)[3] This report shows that among other crimes, there were 86,900 instances of identity theft and identity fraud (which includes impersonation, using of other's identity card, identity theft etc mainly for financial gain),[4] 207,700 instances of financial frauds (which includes losses of plastic cards, bank frauds etc),[5] 137,600 instances of computer misuse (the report does not include virus infections)[6] and 609,700 instances of sexual offences which cover victimization of children mainly.[7] Apart from the Garlik report, we did not find any detailed analysis of cyber victimization, especially of women in UK. This could be an indication as how individuals, especially women are conservative about reporting the online crimes that happen to them. A victimization survey to unearth online crimes against women in the UK is the need of the hour.

7.2 UNAUTHORIZED ACCESS AND RELATED ACTIVITIES

As discussed in chapter 2, hacking and hacking related activities may not always be restricted to crimes committed against the nation or the corporate entities alone. We see it 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 victim etc, are also criminal activities like stalking or bullying. Strangely enough, in UK, these sorts of cyber criminal activities against women have been never given a separate legal treatment on the pretext that these are also one of the hacking related activities which are done to individuals. We feel that the core reason for the growth of internet crimes against women could be lackluster attitude of the law and justice machinery to understand the nature of hacking related activities targeted especially to the women. Such sorts of unauthorized access towards personal data may lead to several other cyber offences including public defamation and humiliation, impersonation, unwanted exposure of the victim in adult entertainment industry etc.

Unlike the US, the UK does not have any women – special regulation to cover cyber offences originating from domestic violence or dating violence; rather the offences related to unauthorized access are regulated by a compact legislation called "Computer Misuse Act, 1990". Under this Act, three offences are penalized, namely, unauthorized access to computer material,[8] or to enable any such access to secure unauthorized access,[9] intention to create further menace with such unauthorized access[10] and unauthorized modification of the computer material.[11] As mentioned earlier, this Act was created to protect both men and women victims. Notably, the drafting of the language could very well suit the needs for preventive actions against harassment of women also when it says that the *mens rea* must be directed to the 'act' that the offender knows would successfully accomplish his intention to harm his victim.[12] In brief, the offender can be held guilty for unauthorized access if it is proved that he used his technological knowledge to access the computer material or data with intention to harm the victim.

The penalties for such offences are on a summary conviction in England and Wales to imprisonment for a term of 12 months or to a monetary fine not exceeding statutory maximum, or both. In case of summary conviction in Scotland, the law prescribes imprisonment for six months or to a fine not exceeding statutory maximum, or both.[13]