

Chapter 4.5

Cyber Laws for Preventing Cyber Crimes Against Women in Canada

Debarati Halder

Centre for Cyber Victim Counselling, India

K. Jaishankar

Manonmaniam Sundaranar University, India

CHAPTER OVERVIEW

This chapter gives an overview of laws related to cyber crimes against in general and women in particular. Though there are no specific laws that were developed to mitigate crimes against women in cyber space, Canadian laws of physical space govern the cyber space crimes well. The various issues that are discussed in this chapter are: Cyber nonsexual offences against women and regulating laws in Canada, Online Stalking and related offences, Online harassment through modification of digital contents and misusing the same, Offensive communication against women, Cyber defamatory libel against women, Cyber hate propaganda against women and legal situation, Responsibilities of the ISPs, Cyber privacy and related offences against women, Regulating cyber sexual offences for women in Canada, and the problem of Obscenity and regulating laws.

INTRODUCTION

The Canadian scenario differs from the US in issues of laws on cyber crime. Canada lacks a consolidated Information technology law. The Canadian cyber crime against women scenario

differs from the UK as well. It was interesting to note that even though Canada has followed British Penal system (which was a model since the late 19th century for almost all the English colonies as well as modern commonwealth countries like India, Australia etc) for covering offline as well as online crimes, the Canadian socio-legal approach towards generalizing various types of cyber crimes

DOI: 10.4018/978-1-61350-323-2.ch4.5

is quite similar to that of the US. Canada has no gender sensitive laws for cyber crimes like that of Women's Reauthorization Act of the US to regulate cyber stalking against women. But at the same time, the governmental efforts to spread awareness through police handbooks about cyber victimization serve similar purposes to a great extent. Notably, Canada lacks statistical data on victimization of women in the cyber space. Hence, in this segment we have tried to analyze the trends of victimization of women in the cyber space only from a legal perspective.

CYBER NONSEXUAL OFFENCES AGAINST WOMEN AND REGULATION OF LAWS

Online Stalking and Related Offences

The Canadian Criminal Code¹ under section 264(1) prohibits harassing activities and prescribes punishment for imprisonment for minimum 10 years or summary conviction.² This particular section was meant to punish offline harassment including stalking and creating fear factor in the victim's mind. The term "stalking" does not find any mention in this Section, however, the characteristics of stalking³ are well depicted in section 264(ii) and they are termed as 'prohibited conduct'. These are:

- a) Repeatedly following the other person from place to place or anyone known to them;
- b) Repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;
- c) Besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or
- d) Engaging in threatening conduct directed at the other person or any member of their family.

Even though this section was mainly framed to deal with offline stalking, it is now being stretched to online stalking and harassments too. The handbook for police and crown prosecutors (DOJ, Canada, 2004) has refined the concept of cyber stalking and online harassment in the meaning of section 264, when used for computer related crimes. The handbook in its opening paragraph under the title of "legislative history of criminal harassment" stated that:

On August 1, 1993, the Criminal Code was amended to create the new offence of criminal harassment. It was introduced as a specific response to violence against women, particularly to domestic violence against women. However, the offence is not restricted to domestic violence and applies equally to all victims of criminal harassment.

The statement indicates how section 264, when used for online stalking and harassment, can protect women's interest. Under Para 1.6, titled "Cyber stalking and online harassment", the Handbook admits that while applying section 264 to cyber stalking, only two requirements of the aforesaid section can be applied, namely (1) Repeatedly communicating with, either directly or indirectly, the other person or anyone known to them, which has been stated in Subsection 2(b), and (2) engaging in threatening conduct directed at the other person or any member of their family which has been stated in subsection 2(d) (DOJ, Canada, 2004). The Handbook further shows three types of 'offline stalkers' which are "erotomaniac stalker", "Love obsessional stalkers" and "simple obsessional stalker" (DOJ, Canada, 2004). It is needless to say that these types of stalkers are now randomly using internet and their activities are more hi-tech. (DOJ, Canada, 2004). Online stalking would necessarily be associated with threatening mails, blackmailing and even offline physical threats. Section 264.1 regulates such threatening conducts with a punishment for 5

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cyber-laws-preventing-cyber-crimes/60980

Related Content

Cloud-ElGamal and Fast Cloud-RSA Homomorphic Schemes for Protecting Data Confidentiality in Cloud Computing

Khalid El Makkaoui, Abderrahim Beni-Hssane and Abdellah Ezzati (2019). *International Journal of Digital Crime and Forensics* (pp. 90-102).

www.irma-international.org/article/cloud-elgamal-and-fast-cloud-rsa-homomorphic-schemes-for-protecting-data-confidentiality-in-cloud-computing/227641

Evaluation of the Attack Effect Based on Improved Grey Clustering Model

Chen Yue, Lu Tianliang, Cai Manchun and Li Jingying (2018). *International Journal of Digital Crime and Forensics* (pp. 92-100).

www.irma-international.org/article/evaluation-of-the-attack-effect-based-on-improved-grey-clustering-model/193023

E-Government, Security, and Cyber-Privacy: Individual Rights versus Government Responsibility

Ross Wolfand Ronnie Korosec (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1314-1327).

www.irma-international.org/chapter/government-security-cyber-privacy/61011

An Audio Steganography Based on Run Length Encoding and Integer Wavelet Transform

Hanlin Liu, Jingju Liu, Xuehu Yan, Pengfei Xue and Dingwei Tan (2021). *International Journal of Digital Crime and Forensics* (pp. 16-34).

www.irma-international.org/article/an-audio-steganography-based-on-run-length-encoding-and-integer-wavelet-transform/272831

Identifying "Hot Link" Between Crime and Crime-Related Locations

Yongmei Lu (2005). *Geographic Information Systems and Crime Analysis* (pp. 253-269).

www.irma-international.org/chapter/identifying-hot-link-between-crime/18828