Book Review on Cyber Crime and the Victimization of Women: Laws, Rights and Regulations

Dr. Pallavi Singh and Radha Ranjan

BOOK REVIEW ON CYBER CRIME AND THE VICTIMIZATION OF WOMEN: LAWS, RIGHTS AND REGULATIONS

Dr. Pallavi Singh[1] and Radha Ranjan[2]

Book Title: Cyber Crime and the Victimization of Women: Laws, Rights and Regulations

Authors: Debarati Halder and K. Jaishankar

Publication House: IGI Global

Year of Publication: 2012

ISBN No.: 978-1-60960-830-9

This book revolves around the concept of Cybercrime with special emphasis upon victimization of the women. The book has been forwarded by Susan W. Brenner NCR Distinguished Professor of Law and Technology University of Dayton School of Law, Dayton, Ohio, USA. It is crafted especially for the women population as there is enormous unequal proportion between men and women when it comes to cybercrimes. Secondly, the impact of victimization is felt more by the women as compared to men. Thirdly, new cybercrimes have come into existence where women are the main victim and fourthly, there has been a paradigm shift in emergence of private policing by the NGOs such as Internet Watch Foundation (IWF), Centre for Cyber Victim Counselling, etc. This book is voluminous spans over ten chapters and ten Appendixes which is stated as below:

---

[1] Assistant Professor of Law, Central University of South Bihar, Gaya
[2] Doctoral Research Scholar, Central University of South Bihar, Gaya

I.   CHAPTER 1: INTRODUCTION

This chapter divides the era of cyber space into email period, chat room period and cyber social networking period. It stresses upon why the book is restricted to the woman audience. It states its methodological approach which is from the purview of criminological, victimological and legal approach to victimization against women in the cyberspace. The aim and audience of this book is providing critical appraisal and perspective to cyber victimization of woman from legal angle. The book is useful for students, practitioners, academicians and police. The scope and expected outcomes of this books is to covers offences committed against women in the online world. It covers majorly non-economic cybercrimes and social crimes serving to the women clientele.

II.   CHAPTER 2: DEFINITION, TYPOLOGY AND PATTERNS OF VICTIMIZATION

The Convention of Cybercrime also called the Budapest Convention was pioneer convention in 2001 which tried to see the cyber crimes from legal angle internationally. The convention divided the cyber crimes into five different categories, i.e. crimes against confidentiality, computer related offences, child pornography, offences relating copyright infringement and abetting or aiding these offences. Numerous definitions of *'cybercrime'* was given by scholars. The authors have also discussed different categories of cybercrimes. There is also a requirement that we need separation operational definitions for every cybercrime committed against women. The cybercrimes against women is divided into three categories: Non-sexual crimes, Sexual crimes and cyber assisted offline crimes.

III.   CHAPTER 3: ETIOLOGY, MOTIVES, AND CRIME HUBS

This chapter analyses the causes for victimization against women. The motives and reasons for committing the cyber crimes against women is also discussed in this chapter. For example: Personal enmity with the

victim due to marriage, relationship and emotional bonding, Sexual obsessions, etc. Characteristics of both the *'victim'* and the *'perpetrator'* is discussed in detail. Victim precipitation theory and Victim turned offender's theory have been resorted as to there are victims who at later stage may turn into offenders due to suppressed anger and revenge taking attitude.

IV.   CHAPTER 4: WOMEN'S RIGHTS IN THE CYBER SPACE AND THE RELATED DUTIES

The authors have highlighted that right for women is not only necessary in physical space but also in cyber space as well. CEDAW, i.e. *Convention on the Elimination of All Forms of Discrimination against Women* as a convention is discussed in detail for women's rights. Comparative analysis is made with U.S., Canada and India in understanding the legal provisions to combat the cyber crimes against women. There are certain duties which the women as netizens are bestowed with is also discussed in detail.

V.   CHAPTER 5: LEGAL TREATMENT OF CYBER CRIMES AGAINST WOMEN IN USA

U.S.A. is one of the countries in the world which pioneered the approach of evolution of internet. It experienced plethora of cyber crimes in response to which they created new laws to combat the same. This chapter explains in detail the different laws were developed to prevent cyber victimization against women in online world. The regulation of cyber bullying, cyber stalking is discussed in depth in this chapter. The aspect of privacy viz-a-viz the different laws related to same has been explained.

VI.   CHAPTER 6: CYBER LAWS FOR PREVENTING CYBER CRIMES AGAINST WOMEN IN CANADA

In depth explanation is provided with respect to cyber crimes against women and in general. In Canada per se, there are no special legislations

or laws which primarily deals with combatting the cybercrimes in the cyberspace. However, laws in Canada for crimes pertaining to physical space extends to crimes committed in the cyber space as well. Various cyber crimes are discussed in this chapter: Online harassment, cyber stalking, cyber defamation, hate speech, obligations of he Internet service providers (ISPs), and how to regulate sexual cybercrimes in Canada.

VII.   CHAPTER 7: CYBER SPACE REGULATIONS FOR PROTECTING WOMEN IN UK

This chapters dwells upon various cyber space regulations in the United Kingdom for cyber stalking and offensive communications. It also emphasises the need for the women centric laws to prevent their victimization in the cyber world. The current cyber laws for the women are considered to be archaic and of rudimentary character. Issues pertaining to consent and non-consent to sexual exposures is also provided.

VIII.   CHAPTER 8: CYBER CRIME AGAINST WOMEN AND REGULATIONS IN AUSTRALIA

This Chapter deals with the legal provisions in combatting cybercrimes against women in Australia. Various cyber crimes are discussed under this chapter ranging from stalking, defamation, harassment, blackmailing to threatening. There a strong need for making new laws in Australia for tackling cyber crimes against women. Also, this chapter ends with a discussion.

IX.   CHAPTER 9: CYBER VICTIMIZATION OF WOMEN AND CYBER LAWS IN INDIA

This chapters is divided into three parameters: Firstly, discussing situational analysis of cyber victimization against women, Secondly, it deals what are the current laws dealing with cyber crimes against women with respect to stalking, hacking, combatting of privacy, voyeurism,

pornography of women in the cyberspace. Thirdly, it deals with what are the various lacunas and loopholes in the present legal framework which is the Information Technology Act, 2000 and what mechanisms can be devised to overcome the same.

X.   CHAPTER 10: MODEL CHARTER AND CONCLUSION

The authors have prepared a model charter to prevent cyber victimization against women. The charter is divided into three parts, Part I: deals with Definitions, Part II: deals with a tentative proposal entailing cyber rights for the women and Part III: Code of conduct in cyberspace. A strong emphasis is also given the need for women centric legislations in both developing and developed nations. The authors ended this book with a saying a much more in-depth research is required in the field of cyber victimization against women.

XI.   RESEARCH GAP AND PATH BREAKING INNOVATION RESEARCH

- This book was written a decade ago. Ten years from now a lot of revolution has taken place in the field of Information and Communication Technology. After the unprecedented wave of COVID-19, zoom bombing is born. As per Harvard University, zoom bombing is defined as: *"A new term, "Zoom Bombing," is when people who have not been invited enter Zoom meetings to cause disruption. Such disruptions can be mild, or as we've seen elsewhere, can include racist, hate, or pornographic material."* Such crimes don't find the place in this book.
- Furthermore, the extent of the book's covering of the subject matter may be limited. Given the ever-changing nature of cybercrime and digital technology, it is critical to keep up with the most recent advances and new risks in the domain of cyber victimisation. A lack of recent material may make the book less relevant to people seeking current expertise in this topic.

The relationship between cybercrime and the victimisation of women is examined in depth and with insight in "Cybercrime and the Victimisation of Women: Laws, Rights, and Regulations," written by Debarati Halder and K. Jaishankar. The writers provide a holistic view of the obstacles women encounter in the digital sphere and the legal tools at their disposal by carefully examining legal frameworks, case studies, and sociocultural factors. The way in which Halder and Jaishankar examine the many dimensions of female cybervictimization is among the most interesting things about their work. The writers discuss the various types of digital abuse that women experience and the negative effects it has on their safety, rights, and general well-being. These include financial fraud, revenge porn, and online harassment and cyberstalking.

The book also critically assesses the rights, laws, and rules that now regulate cybercrimes against women, pointing out both the advancements and the continuing shortcomings in providing victims with adequate protection and redress. Halder and Jaishankar provide insightful information about the advantages and disadvantages of legal frameworks at the national, regional, and global levels through in-depth case studies and comparative analysis. The authors also urge a comprehensive strategy that includes victim support services, awareness-raising campaigns, capacity-building activities, and legislative changes to address the issue of women being victimised online. They emphasise the necessity of a coordinated approach to prevent gender-based cyber violence by highlighting the significance of cooperative efforts including government agencies, civil society organisations, and technology corporations.

Finally, "Cyber Crime and the Victimisation of Women: Laws, Rights, and Regulations" is regarded as a foundational text in gender studies and cyber law. For legislators, attorneys, academics, and activists promoting gender equality and digital justice, Halder and Jaishankar's thorough analysis and their useful suggestions for legislation and practice make this book a

must-read. Their work is a current and useful resource for directing future study, advocacy, and action in this crucial area as we try to create safer and more inclusive digital environments for women.