



Irina Nagornaya

Cybercrime and the Victimization of Women: Laws, Rights and Regulations

Halder D., Jaishankar K.¹

D. Halder is an advocate and a legal scholar. She holds a position of the managing director of the Centre for Cyber Victim Counselling and of the Vice President of Working for Halting Online Abuse (WHOA, USA).

K. Jaishankar is Doctor of law (PhD). He is a senior assistant professor in the Department of Criminology and Criminal Justice at Manonmaniam Sundaranar University in Tirunelveli (India), the founding president of the South Asian Society of Criminology and Victimology, the founding executive director of the Centre for Cyber Victim Counselling.

The book consists of a foreword, preface, ten chapters and ten appendices containing the sections of applicable legislation.

In the first chapter "Introduction" the authors explain why women`s victimization in cyberspace should be scrutinized separately:

1. Statistics of WHOA show that the majority of victims of cybercrimes are women (p. 4).
2. Cybercrime has a greater adverse effect on women than on men. According to the authors, due to such offenses women feel humiliated; libel and disclosure of confidential information can cause stigmatization and undermine the reputation of woman (p.5).

Unfortunately, we should agree with the second point: women are often more vulnerable than men, even in the developed countries.

In the second chapter "Definition, Typology and Patterns of Victimization" the authors analyze existing definitions of cybercrime and give their own definition - crimes committed against individuals or groups of individuals to undermine the reputation of the victim, to inflict physical or mental harm, directly or indirectly, by using modern telecommunication networks such as the Internet (chat rooms, emails, pages ads and virtual teams) and mobile phones (SMS and MMS) (p. 15).

The third chapter "Etiology, Motives, and Crime Hubs" describes factors contributing to the increase of cybercrimes including the ability of offenders to use pseudonyms, women behavior in cyberspace (for example, visiting sites with sexual content), failure to report about cybercrimes to the authorities.

Motives of cybercrimes against women include personal enmity; professional jealousy; sexual motives; self-affirmation; wish to defend the particular point of view, as well as to test skills and knowledge of Internet technologies.

¹ Hershey, PA, USA: IGI Global, 2012. – XII+264 p.



In the fourth chapter “Women’s Rights in the Cyber Space and the Related Duties” the authors refer to art. 17 of International Covenant on Civil and Political Rights (1966) which prohibits “arbitrary or unlawful interference with privacy, family, home or correspondence, or unlawful attacks on honour and reputation”. European Convention on Cybercrime also contains many important rules.

However, the authors believe that it is necessary to adopt a comprehensive act to protect the rights of women in cyberspace. They convinced that the majority of cybercrimes are committed because of the absence of such legislation.

In subsequent chapters, authors discuss the criminal law protection of women’s rights in the virtual space in common law countries (USA, Canada, UK, Australia, India). This part of the book is very useful as it not only provides information about the criminal legislation of these countries but also about the ways of its development.

Let’s examine the criminal law protection of women’s rights on the virtual space in India.

Section 66A of Information Technology Act on 17.10.2000 N 21 (as amended on 23.12.2008) prohibits sending by means of a computer resource or a communication device any information that is grossly offensive or has menacing character, or persistently sending any false information for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will. It is also punishable to send any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

Section 66E outlaws capturing, publishing or transmission of the image of private area of any person without his or her consent. Section 67 provides punishment for publishing or transmission obscene material in electronic form.

Section 509 of Indian Criminal Code prohibits words, gestures or acts intended to insult the modesty of a woman.

The authors emphasize that the Constitution does not guarantee the freedom of speech in the case of indecent behavior.

The authors believe that the laws of the considered countries are not able to protect effectively the rights of women in cyberspace. Therefore, in the tenth chapter they offer their own draft of Model charter on preventing the victimization of women in the virtual space, which consists of three parts.

Part 1 contains basic concepts, defines various cyber offences.

Part 2 fixes women’s rights in cyberspace including rights to:

- protection from all forms of discrimination;
- safety and dignity;
- the freedom of speech and expression ;
- information in cyberspace;



- communicate with others;
- block unwanted contacts;
- conduct their business through the Internet.

Part 3 fixes the duties of Internet users: to respect the personal privacy of others, to refrain from obscenity and offensive language, from modification and re-publication of personal data without the consent of the authorized person.

The authors suggest that international organizations, including the UN, as well as scientific organizations should continue to study the behavior that infringes the rights of women in cyberspace. It will help to improve existing legislation in order to protect women as the most vulnerable social group.

Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. [4] Obama, B. (2014). Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1), 1-20. [8] Clay, W. (2005). *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service Report for Congress. Retrieved from <http://www.dtic.mil/dtic/tr/fulltext/u2/a444799.pdf> on 27-12-2017.