International Journal of Academic Research
ISSN: 2348-7666 Vol.2, Issue-3(1), July-September, 2015

Victimisation of women under Cyberspace in Indian Environment

Dr. S. K Mohapatra, Reader, P.G Department of Law,
Sambalpur University, Odisha

Abstract

This research study provides a review and analysis of the development of regulatory instruments (statutes, recommendations, guidelines, etc.) to protect privacy and related interests with regard to the processing of personal data of women in cyberspace. Taken together, these instruments form a field of law and policy that has attained considerable maturity, spread and normative importance over the decades. The awareness of the individuals regarding the law and policy in this concern is the prime objective and which will reflect the status of India. Enveloping the regulatory field is an immense body of academic commentary analysing privacy and data protection issues in cyberspace from a variety of perspectives.

Keywords: Cyberspace, Privacy, Technology, Feminism, Law & Policy

Introduction

Under this technological development era the most effected victim is women. Every sphere of life now a day, start and end with digital intervention i.e. computer technological interferences. In the light of this, the positive as well as negative sides also come out. Cybercrime is a global phenomenon. The advancement of technology, cybercrime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. The privacy and personal security of the individual are under threat with this growing issue of cybercrime in the cyberspace. Internet is world's largest information system and giant network. As telecom infrastructure developments continue to penetrate into smaller towns, Internet usage numbers showcase the effects with its ever increasing base of users. The Internet is now a part of the globalization process that is evidently sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a "compact" world. The cyberspace has been a blessing to human civilization. Internet has connected people around the globe. The desire to know what is unknown is indispensable of human nature. It is the desire to know about the people, who inhabit the earth, has aggravated the urge of discovering the untraded path. This has led to the unearthing of the cyber world. One of the benefits which internet has provided to every section of the society is empowerment, [1].

The social networking websites (SNWs) have developed a new arena for socializing. Irrespective of any distinction, women in the society are exulting with this liberation to the fullest. From online shopping to net banking, from e-ticketing to e-tax filling, it has made the life of Indian women easy[2]. It has enabled women to fight for equality even within the confines of their society. They can now share their experiences to the whole world, and this advantage of being able to share their success stories as well as their problems have given them a platform in the global world. Along with providing them with a platform to voice their struggles and success in life, it inscribes new spaces of power, which is accompanied with knowledge.

Ironically, on the one side, the internet is serving as boon, but on the other side, it has made the life of women insecure due to rising cybercrime in the virtual world. Women of all ages and milieu are in jeopardy with the coming up of internet[3]. While many women are victimized online, what makes Indian women unique? India is predominantly patriarchal and orthodox country and women who are victimized are mostly blamed and online victims are no exception[4].

Similarly, the penetration of Information and Communication technologies (ICT) offers great including women opportunities and more and more users are getting connected. The cost of owning Internet enabled devices has also facilitated to this growth. The increase in penetration of ICT, has spurred a growth in ICT-based businesses and services. The ICT sector with its direct and indirect contribution to various socioeconomic parameters has become one of the most significant growth catalysts for the Indian economy. Besides transforming India's image to that of a global player as provider of world class ITES enabled solution and services, this sector is also significantly influencing the lives of thousands of people on various parameters like employment, standard of living and diversity among others. It has embarked on various IT-enabled initiatives like Government to citizen services, public distribution systems, Healthcare, e-Learning, and mobile banking, etc.[5]

This research paper deals with the basic conceptions and legal regulations that protect Indian women in cyber space. There are various issues that are discussed briefly in this paper are: Cyber harassments including hacking and hacking related offence against women and regulatory provisions, Stalking women and the concerned laws, Harassments, threatening, blackmailing, defamation and related laws. The gap between the technological advancement and legal action are being considered here as a matter of discussion. In this paper as strong emphasis is made on the need for new laws that will protect Indian women in cyber space as a serious lacuna is found in this issue.

Basic Conceptual Impression

The concept of cybercrime is not so much different from that of conventional crime as both include conduct, which cause breach of rules of law. The definitions of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Certain definitions are required for the core of cybercrime acts [6] . Cybercrime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime. The Oxford Reference Online defines 'cybercrime' as crime committed over the Internet. The Council of Europe’s Cybercrime Treaty uses the term “Cybercrime” to refer to offences ranging from criminal activity against data to content and copyright infringement. Thomas and Loader define cybercrime as “computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks”[7]. Schinder define cybercrime as “a subcategory of computer crime and it refers to criminal offenses committed using the internet or another computer network as a component of the crime” [8] . Schell and Martin defined cybercrime as a crime related to technology, computers and the internet and it concerns governments, industries and citizens worldwide where cybercrime takes the form of either piracy, phreaking (obtaining free telephone calls), cyberstalking, cyberterrorism and cyber pornography. Schell and Martin define cybercrime broadly as “a crime related to technology, computers, and the Internet” [9] . Milhorn, on the other hand, simply defines cybercrime as any activity that uses the internet to commit a crime[10].

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. Cybercrime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet.

In India, cybercrime and victimization in the cyber space had remained a subject of great trepidation, but lacks awareness. Bizarre combination of nature of attacks; ever changing trends of the victimization, limited knowledge about direct laws which address cybercrimes in India and rights of victims in cases of cyber-attacks, contribute greatly towards forming a weird approach to cyber victimization scenario. There are millions of internet users in India now who are frequenting the cyber space on a regular basis for professional, commercial, socializing and educational purposes. Since the IT sector in India have seen a boom in the 1990’s, (which still continues), almost every household falling in the economic zone of moderate income groups to high income groups, have internet access at home and people from the age group of 13 to 70 years, belonging to these clusters, are regularly using the internet either at home, or at work places, or at educational institutes, or at cyber cafes. But along with internet-dependency, victimization of ‘cyber citizens’ and also of those who are not in the ‘internet’, have grown in an alarming rate, in spite, India has an exclusive legislation dedicated for information technology, e-governance, e-commerce and also e-socialization to a certain extent; this has hardly helped in curbing the ever increasing victimization of individuals in the cyber space in India.

Sadly enough, less awareness brings in more victimization and cyberspace victimization is no exception. In India, awareness of cyber victimization has remained limited to several informative and useful tips on how to save one’s personal computer and personal data from identity-frauds, emotional blackmailers etc. A comprehensive empirical survey on this issue is the need of the hour.

Legal Status in India: Even though India is one of the very few countries to enact IT Act 2000 to combat cybercrimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the security of women in general is not covered fully by this Act. Cyber bullying can affect everyone, including children. Safety Web provides support for parents to improve internet safety for kids.

Provisions of the IT Act 2000 relating to cybercrime and offences against women in India and the loopholes of the said Act:

Unfortunately even though Chapter XI of the IT Act deals with the offences such as Tampering with computer source documents (s.65), Hacking with computer system (s66), publishing of information which is obscene in electronic form (s.67) Access to protected system (s70), Breach of confidentiality and privacy (s. 72), Publication for fraudulent purpose (s.74) IT Act 2000 still needs to be modified. It does not mention any crime specifically as against women and children.

The elementary problems, which are associated with Cyber-Crimes, are Jurisdiction, Loss of evidence, Lack of cyber army and Cyber savvy judges who are the need of the day.

Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela high Court has accepted through an email. Today with the growing arms of cyberspace the growing arms of cyberspace the territorial boundaries seems to vanish thus the concept of territorial jurisdiction as envisaged under S.16 of C.P.C. and S.2.of the I.P.C. will have to give way to alternative method of dispute resolution.

Again, under no section in IT ACT 2000, Obscenity personal viewing is an offence, in fact like in IPC 292 again if it is proved that you have published or transmitted or caused to be published in the electronic form only then under Section 67 it can be an offence. Last but not the least, the IT Act 2000 does not mention the typical cybercrimes like cyber stalking, morphing and email spoofing as offences. Mainly these are the provision which are taken care this kind of cybercrimes in cyberspace.

Gap between Legal Actions & Technological Advancement

One of the main reasons behind the increase of cybercrimes against women in India is the less legal protection[11]. Halder and Jaishankar, in their book "Cyber Crime and the Victimization of Women: Laws, Rights and Regulations", have said that, "The issues of women's rights in cyber space could be contributed largely to the sluggish modes of the governments in executing the gender equality and gender justice promises made by the States in the form of fundamental rights" [12],. They have also reported in India cyber gender harassment is often seen as "less important sexual harassment"[13].

Laws related to cybercrime in different countries like Canada, Australia, USA, UK, India etc. are mainly associated with the augmentation of e-commerce, and for this reason,the laws mainly covered commercial and financial crimes, which include hacking, deception etc. Some laws have been designed for email spoofing, cyber-sex, trespassing into others' privacy etc.[14]. However, the laws related to cybercrime against women are correlated to sexual crime and abuses on the internet, but there are many practical difficulties associated with punishing the miscreant. Primarily, many women are not aware of the laws against cybercrime[15]. The report presented by CCVC has also shown that among the 73respondents 80.8% has no knowledge of the fact that cyber stalking, cyber bullying, sending threatening mails etc. if reported are penalized [16] .Moreover, among women only 8.3% has reported to the police. If a crime is not reported, no action can be taken against it. This alsoresults in increase of cybercrime against women as the miscreant's goes scot free.

In 2008, Indecent Representation of Women (Prohibition) Act was shaped mainly to deal with representation of women, which perhaps do not come under the scope of 'obscenity.' Halder [17] puts forth that, "It is definitely a welcome move as India mayget a law focused solely on the victimization of women through indecent portrayal, but at the same time, the concept of indecent representation of women must be freed from patriarchal meanings of social value and morality". Her words again prove that the mindset of people needs to change in order to bring altercation in the position of women and to grant justice to the victimized women.

Apart from the legal gap the provision of anonymity by the cyber space is a reason for the victimization of women [18]. The cyber world is a virtual space where it becomes very easy for the perpetrator to manipulate his identity and hide. The reason behind it is that even if the source from which the offensive matter has been posted can be detected, the police find it difficult to trail the offender. The culprit uses the information from the matrimonial or job sites where peoplegive their credentials for better prospect and this information also makes them a victim. This can be precisely explained by the Space Transition Theory of Jaishankar [19]. According to this theory, "Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime" [20]. Further, Balakrishnan [21], the then Chief justice of India, opined:

> *"The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. Websites are created and updated for many useful purposes, but they can also be used to circulate offensive content such as pornography, hate speech and defamatory materials. The widespread circulation of such content is particularly harmful for women. The pervasive gender discrimination in our society is further heightened since the digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behavior since it is presumed that they will not face any consequences."*

According to Griffiths [22], there are mainly three types of relationships those are prevalent through internet. The first type of relation is generally between people, who never meet and enjoys sexual talk over net. This kind of relationship is normally short lived and the cyber partners may even have real life spouse. They most of the time do not consider the online sexual relationship as being disloyal to their spouses. The second type involves people, who meet over net, but ultimately wants to maintain their relationship offline by meeting, exchanging letters, gifts etc. And the last form of online relationship engages people, who also get connected through internet, but maintain their relationship online for years only because they may be separated from each other owing to their belonging to different countries and can meet very rare. This type of relationship is most difficult to maintain because the two people must have the ability to afford their relationship on monetary grounds[23].

Conclusion

For the purpose of justifying the intention of this research work the concluding statement is being dealing some issues. Like Indian women natives are still not open to immediately report the cyber abuse or cybercrime. The biggest problem of cybercrime lies in the modus operandi and the motive of the cybercriminal. Cyber space is a transit space for many people, including offenders. While people do not live in cyber space, they come and go like any other place. This nature provides the offenders the chance to escape after the commission of cybercrime. Many websites and blogs provide security tips for the safety of women and children in the net. But still then cyber-crimes against women are on rise. The scenario of cyber victimization in India needs to be studied in detail. It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. Most ISPs and social networking sites adhere to western cyber cultures and cyber rules and regulations which may give rise to opportunities to experiment with the personal freedoms, especially freedom of speech and expression and right to privacy. In the Indian social value system, some of such cyber cultures may give rise to severe abuse of fundamental rights guaranteed by our constitution. Matured adult internet users must understand that what is offensive in the real space, must be maintained as offensive in the cyber space also. Cyber socializing has opened the gateway to a global village which may form its own culture, rules and ethics. But that in no way should encourage abuse of personal rights and freedom.

References

[1] Halder, D., & Jaishankar, K. Cyber socializing and victimization of women. Temida, 12(3), 5-26, (2009).

[2] Ibid

[3] Ibid.

[4] Halder, D., & Jaishankar, K.. Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offenders, 6(4), 386-398, (2011).

[5] Anand K Shrivastav & Dr. Ekata, ICT Penetration and Cybercrime in India: A Review, International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 3, Issue 7, ISSN: 2277 128X, (2013).

[6] United Nations Office on Drugs and Crime,Vienna, “Comprehensive Study on Cybercrime”, February 2013

[7] Thomas, D and Loader, B, “Cybercrime: Law Enforcement, Security and Surveillance in the Information Age”, London: Routledge, (202009).

[8] Debra Littlejohn Shinder, "Scene Of The Cybercrime: Computer Forensics Handbook”, (2002).

[9] Schell, B. & Martin, C, “Cybercrime: A Reference Handbook”. Santa Barbara: ABC-CLIO, (2004).

[10] H. Thomas Milhorn, Cybercrime: How to Avoid Becoming a Victim, Universal Publishers, (2007).

[11] Halder, D., & Jaishankar, K. Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global (2011).

[12] Halder, D., & Jaishankar, K. Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global. p. 56, (2011).

[13] Ibid, p. 10.

[14] Citron, K. D, Law’s expressive value in combating cyber gender harassment, MICHIGAN LAW REVIEW, 108, 373–415, (2009). And See also; Halder, D., & Jaishankar, K, Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offenders, 6(4), 386-398, (2011).

[15] Halder, D., & Jaishankar, K, Cybercrimes against women in India: Problems, perspectives and solutions. TMC Academic Journal, 3(1), 48-62, (2008).

[16] Halder, D., & Jaishankar, K, Cyber victimization in India: a baseline survey report. Tirunelveli, India: Centre for Cyber Victim Counselling, (2010).

[17] Halder, S., & Choudhuri, S, ComputerSelf Efficacy and Computer Anxiety of Trainee Teachers: Issue of Concern. Proceedings of episteme, 4, India, (2011) Retrieved on 7th September, p. 28, (2013).

[18] Citron, K. D, Cyber civil rights. boston university law review, 89(61), 69–75. (2009). and See also Citron, K. D. (2009). Law’s expressive value in combating cyber gender harassment. MICHIGAN LAW REVIEW, 108, 373–415.

[19] Halder, D., & Jaishankar, K, Cybercrimes against women in India: Problems, perspectives and solutions. TMC Academic Journal, 3(1), 48-62, (2008).

[20] Ibid, p. 293.

[21] Balakrishnan, K. G. Speech at Seminar on ‘Cyber Crimes against Women’ - Public awareness meeting, Maharaja College, Ernakulam, p.1, (2009). http://supremecourtofindia.nic.in/speeches/speeches_2009/seminar_-_cyber_crimes_against_women_1-08-09.pdf. (Accessed on 1st march , 2015).

[22] Griffiths, M. D. All but connected (Online relationships). Psychology Post, 17, 6-7, (1999).

[23] Ibid.