

Volume 10, Issue 1, (Special Issue)
March, 2018

ISSN No.:2348-4667

Anthropological *Bulletin*

a peer reviewed international journal

Special Issue:
Women and Children's Perspectives

Guest Editor:
Daud Salim Faruque

**A
B**

Department of Anthropology
University of Lucknow, Lucknow, India

Cyber Crime against Women in India: Issues and Challenges

Syed Fahad Hussain¹ and Mohd Shawez Raza²

Information technology has expanded and grown over the past two decades. It has become the axis of economic and technological growth today. The Community of the Internet provides all users with the knowledge they need the quickest networking and exchange platform, making it the most efficient source of information. With the various advances of the Cyber, Internet-based violence has since significantly expanded its roots in both ways. Cyber-crimes represent a significant threat to people. Cybercrime is a worldwide epidemic and women are the soft focus of this modern form of crime. This paper discusses cyber-crimes and the susceptibility of women to online security. Cyber-crime is developing as a threat to nationwide and fiscal stability. Cyber Criminality is a troubling new development that is evolving on the scene in contrast to the broad reach of cyber use. This paper is also an attempt to build an understanding of cybercrime against the women and its forms and suggest various measure to netizens to counter it legally.

Keywords: Information technology, Women, Cyber Crime and Internet User.

1: Introduction

In India, 'cybercrime against women' has been a topic that few have thought about and few have concentrated on it. Thus, a growing range of victims has suffered vulnerably. The word 'cybercrime against women' in India is often cast-off to depict sexual offences and sexual exploitations on the Internet, such as morphing an image and using it for pornographic tenacities, bullying women with sexual blackmail/bullying emails or texts, etc., or cyber stalking. This is too apparent from the circumstance that the common of the cases reported to the police are attentive of the nature of sexual crimes. Several of them have been sentenced under the erstwhile Section 67 (which was intended to protect pornography and obscenity on the web) of the Information Technology Act, 2000. The following examples depict the situation on this issue:

Furthermore, in case of 'Sex Physician,' the convicted, an orthopaedic surgeon called Dr Prakash, was charged and convicted as mentioned in section 506 (Part II of the Section which prescribes penalty for indictable offences for death or severe injury), Section 367 (which communicates with kidnapping or kidnapping for death or serious injury) and Section 120-B (criminal conspiracy) of the IPC And Section 67 of the Information Technology Act; Doctor Prakash was accused of taking obscene photographs and videos by pressing women to commit sexual activities and then downloading and circulating these videos as adult movie materials abroad. He was penalized to life in prison and monetary fine by Rupees. 1.25.000, according to the Unethical Trafficking Act, 1956 (Debarati Halder, 2012).

¹ Research Scholar, Department of Social Work, Aligarh Muslim University, India.
hussainfahad81@gmail.com

² Research Scholar, Centre for Women's Studies, Aligarh Muslim University, India.

As in case of the State of Tamil Nadu vs Suhas Katti, which would be considered to become one of the initial cases to be reported under the Information Technology Act, 2000 (IT Act), the convicted Katti posted libelous, slanderous messages regarding a divorcee in the Yahoo message group. The accused has declared that the accuser is the one who demands for sex. The accused was charged according to sections 469, 509 of the Indian Penal Code (IPC) and 67 of the IT Act 2000 and sentenced to two years of strict imprisonment and fine. The United Nations defines violence against women as 'any act of gender-based violence that contributes in or is likely to result in, physical, sexual or emotional injury or trauma to women, includes threats to such activities, coercion or unreasonable deprivation of liberty, whether in public or private life.' (Debarati Halder, 2012).

The cases mentioned above were the first of its kind to have been reported in India following the entry into force of the IT Act 2000. Swapna Majumdar opined that violence toward women is not cultural or regional; it intersects cultures and groups. Disconcerting as it is, the irony is that violence against women has now become an inevitable standard of living, because women accept violence as part of their married life before it becomes intolerable. (Majumdar 2003). The violence is changing its forms from home to internet because of the male dominated Indian society. The state of violence against women is becoming more frightening day by day, with its expanding forms. Abuse has today occupied on a new dimension toward women, as it is evolving as of the knowledge called cyber abuse that is the critical subject of this paper. The frequency of online violence against women in India is very tall and is suspected to be on the rise.

1.1: Definition of Cyber Crime:

Indian law does not include an adequate description of cybercrime in any statute, and neither does the Information Technology Act, 2000; it doesn't describe cybercrime as cybercrime. In general, however, the term cybercrime relates to any criminal behaviour carried on or with the help of digital technology or computers. Debarati Halder and Dr K. Jaishankar define cybercrimes as:

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

2: Methodology

The present review is descriptive and aims to explain the current state of cybercrime toward women. All data is gathered from several secondary sources, such as books, journal articles and publications, domestic and foreign studies, newspapers and magazines. The information obtained is evaluated using a thematic analysis approach to enhance the credibility of the findings.

3: Cyber violence and victimization against women in India

Since the 1990s, the information technology segment in India has perceived a paradigm shift which continues. Practically every family with reasonable economic conditions has admittance to the internet. In other words, the Internet had turned the concept into our living rooms. Users from 13 and 70 years of age who've had internet access are continually using it, whether at work or home, in cyber cafes, in public universities, etc. Jyoti Rattan's study indicates that 60% of all websites have sexual content. Twenty per cent of them asked their guests, 13 per cent went on a volunteer basis, and the rest were painted. The widespread availability of chat rooms and the susceptibility of personal data to unauthorized access render women and children the simplest victims in the field of Cybercrimes Jeet, S (2012). Halder and Jaishankar (2008) conversed ten necessary forms of cyber-crimes that

happen to Indian women in cyberspace. These include: e-mail harassment, cyber-stalking, cyber defamation, hacking, morphing, e-mail spoofing, cyber-pornography, cyber-sexual defamation.

4: certain forms of cyber offences against women:

1: Cyber Stalking: Cyber Stalking is the usage of the Cyberspace or other electronic means to harass or threaten a person, a group of individuals or an organization which can include making false allegations or claims of fact, monitoring, threats, identity theft, damage to software or devices, and seeking sex from minors, or seeking evidence that can be used to threaten them. It is among the most spoken about cybercrimes typically perpetrated targeting women and kids abused by men, sexual abusers or perverts. Mostly, cyber-stalker victims are new to the web and unfamiliar with the laws of Internet usage and security. There are four causes for cyber-stalking, namely sexual harassment, revenge and hate, love obsession, and ego and control. Women are targeted via websites, discussion boards, chat rooms, blogs, emails, etc.

2: Cyber Defamation: Another prevalent web crime against women is cyber abuse, including slander and defamation. It evolves by publishing libelous and misleading details or sending a mail containing defamatory data to all people's friends (Agarwal 2013). The 2010 survey CCVC (Centre for Cyber Victim Counselling) shows that 71.7 percent of cyber as well as offline defamation exists due to cyber defamation.

3: Cyber Pornography: one more form of online threat to women's protection. Well, thus according A.P. Mali, "The graphic, sexually explicit subjugation of women through images or words that very often includes pornography is verbal or pictorial content that depicts or explains sexual activity that is degrading or abusive to one or more of the participants in such a way as to support degradation. The person who has chosen or consented to be hurt, violated or subjected to exploitation does not alter the degrading character of such actions "(Mali 2011). According to the IT Amendment Act 2008, the offence of pornography referred to in Section 67-A, anyone who publishes and transmits or allows to be published and circulated in electronic form any content that includes sexually suggestive activities or actions can be referred to as pornography. As per sections 292/293/294, 500/506 and 509 of The Indian Penal Code, 1860, is also applicable and the claimant can file a report near a police station where the crime is committed or if the crime has been recorded. Since an offence has been identified, the convicted will be called as the first conviction for a period of imprisonment. That can go up to a fine that can amount to 10 lakh Rupees over a five-year term.

4: Cyber Harassment via Emails: Abuse of female internet users via e-mails is not new-fangled in the world of the internet, which might include an offensive message on the wall of accounts and personal e-mail I-d displayed on the profile, frequent visitor peeling and leaving a message on her wall, sending a plea for friendship, continuously sharing messages that disagree with her and entering groups where she is a member. Besides, abuse involves abuse, chanting, bullying or stealing, etc. via e-mail. E-harassment is close to that of the mail Harassment or felony but also causes problems when it is uploaded from false IDs or cloned accounts, etc. intending to terrorize, bullying, abuse, abusing, insulting or denigrating female netizens (Agarwal 2013).

5: Email Spoofing It: Send email to another person so that someone else seems to have got the email. It is so common that the email we receive is actually from the person identified as the sender (Mali 2011). It's not acknowledged anymore. In the 2010 CCVC survey, hate mails from different people came from 41.7 percent, and sexual or female thinking came from 45.5 percent. On the opposite, just 8.3 percent want to go to the police.

6: Cyber Morphing: This crime is comparable to incest, and we can even claim cyber obscenity. Photographs of female participants are taken from their private photo album. They are altered for adult purposes by using portions of the images, such as the skull and up to the breast (Halder and Jaishankar 2009). Female images stood accessed through fraudulent handlers and repositioned on various internet site by making bogus accounts after they have been morphed. This is a defilement of the Information Act 2000 and is the subject of Sections 43 and 66 of that Act. It can similarly be booked under the Indian Code of the Panel (Agarwal 2013). The absence of knowledge of these types of offences allows the perpetrator to make this mistake.

7: Cyber Hacking: In this type of cyber violence, some specific targets are chosen to hack their social media accounts and use their info for criminal purposes. Also, the drudge can make open invitations to have sexual activity with the owner of the profile at her Residence (Halder and Jaishankar 2009: 13). According to Sections 43(a) and 66 of the IT Amendment Act, 2008 and 379 and 406 of the Indian Criminal Code apply for reprimand afterwards, the cyber hacking legislation has been violated. Under the IT Act, the convicted person will be liable for captivity and punishments extending up to 3 years and five lakh rupees or both if the crime remains confirmed. The crime is morally reprehensible, evident, and aggravated by the sanction of the appreciated Court where an inquiry into such an offence is still ongoing and subject to trial by any judge. (Mali 2011)

8: Virtual cyberspace rape: This is another form of aggressive and brutal cyber-marginalization that targets women in the social media world with scumbags or harassers. Moreover, it posts profane communications such as, "I am going to rape you," "I am going to tear you up," your social media profile will be f ... ed off "and so on, or some community members can" crowd attack "the embattled female with arguments that effectively create more excitement amid other unconnected members to express an opinion on the target's sex. Then the owner of the profile becomes a hot problem with filthy titles, sexual chats, pornography etc.

These are some of the most commonly debated ways of cyber victimization against women in cyberspace that typically take place in our extremely-macho culture. Besides, cyber victimization includes cyber bullying, hacking, phishing, cyber-fire domestic harassment, impersonating, blackmailing, etc. Maltais (2005)

5: Conclusions of the Cyber Crime Victimization Report 2010.

- Most people do not assume that it is essential to read the policy rules, terms and conditions of the networking websites before entering into a contract with these sites and thus opening their accounts.
- Some people do not mind sharing their profiles or accounts and passwords with wives and children.
- Several individuals want to engage in prevalent cyber socialization and are non-aware of junk or phishing electronic mail, etc. Many individuals are ignorant of simple cyber ethics.
- As we observed, the Indian value social structure varies from that of the U.S.A and European nations. Indian users are seeking to incorporate Spaghetti western cyber ethos through their peculiar societal value structure, which allows the most prominent challenges through cyberspace to emerge. That is why cyber defamations, harassing words, sending offensive tweets, etc. to Indian internet handlers are becoming rampant. Voluptuous offences on the Cyberspace are therefore on the rise.
- Social media platforms like YouTube and Twitter are often used to bully females. However, most people don't grasp the actual reality of Internet abuse.

- Several people are well aware of the intrusion, and very few take steps to protect himself from hacking. Correspondingly, it has already been noted many are aware of security crimes that can lead to criminal issues. However, perhaps the maximum internet penetration rate in India is not conscious that cyber stalking could also lead to criminal activities.
- Only a few people, particularly women, choose to report victimization to the police because they feel like this might lead to further marginalization.
- Women are particularly vulnerable to psychological distress than men in cyberspace. "Most women receive mail from unknown men with troubling details, invites from friends, words of harassment, etc., and that might be the product of data gathering. Furthermore, they are also victims of a variety of forms of abuse perpetrated by their former partners, including former colleagues.

6: Suggestions and steps to block cyber crimes:

Women also need to be conscious of cyber victimization on their own, depending on the legal system against cybercrimes, because the time has come to refuse to accept silence. Furthermore, Internet regulations are not widespread, as they vary from nation to nation. Currently, each user desires to glance the web secretly and securely, particularly for females. We need to take certain action to fix this problematic Situation. Now are several phases and ideas as to how women can protect themselves from being abused in cyberspace and in what way they can make their online views and interactions harmless. Kumar,T& ,Jha,R (2012)

- **Adjust PINs from time to time:** In reality, every user just prefers simple to remember passwords because it is more comfortable. If you want to reduce the risk of Internet crime, changing your password is a great way to make your data and social networks more secure and difficult for cybercriminals to access (Pennelli 2012). Baffling or tricky password covers all accounts, including mobile phones, emails, landlines, insurance, credit cards, etc., and it's impossible for someone to guess. And hidden questions cannot be answered quickly (Moore, 2009). Secure passwords include letters, numbers and symbols. Evirate words that are in the dictionary and some relevant dates, and use different codes for different domains (Online Privacy & Protection Tips 2010). However, updating your password can be very useful to keep your privacy secure.
- **Stop sharing a home address:** This is a framework, especially for women who are and are highly visible business executives. You can rent a private mailbox or use their working address. It can then help them out.
- **Keep social relationships secure:** This is also the problem that everybody needs us to think that we should have two thousand mates. Dunban's number⁷ indicates that a person should have a good social relationship with a small number of men and a maximum of 150. We certainly don't need those two thousand Facebook fellows, because we probably can't know more than 150 of them mentally. Holding a limit on the number of people would ensure that we would get our information to people you encounter and to people that you don't encounter very well (Pennelli 2012). Women should get rid of inappropriate friendships.
- **Education drive against cybercrimes:** A grassroots awareness movement such as classrooms, collages, etc. on cybercrimes such as hacking, economic theft, defamatory practices, abuse of e-mails and social networking platforms, computer harassment, online pornography, e-mail bluffing, etc. (Halder and Jaishankar 2010: 22). These movements may be useful in paralysing cybercriminals. 2010 Jaishankar: 22).

- **Seminars and workshops to increase knowledge of cyber victimization:** Police department, lawyers, social workers and NGOs essential to be welcomed to educational organizations, groups, business offices, awareness-raising programmes, meetings and workshops to address the legitimacies and illegitimacies of cyber activity by grownups, including both sexes. Reportage of cyber victimisation straight to the police and NGOs working on internet crimes at all level's duty be promoted. Second, courses and lectures must be held for police officers to develop a more excellent knowledge of those forms of victimisation and to respond effectively to grievances. Scholars and legal specialists, nongovernmental organizations, etc. must engage in such conferences and seminars. (Halder and Jaishankar, 2010: 22).
- **Rigorous and strict rules:** government regulations on cybercrimes must be tighter and tougher in cyberspace. The present Indian Information Technology Act incorporates quite a few sections on cyber threats, particularly against women.
- **Understand the privacy settings in social networks:** Social media platforms and other internet content and facility providers all have confidentiality policy and secluded settings. Everybody must learn to grasp privacy policy then follow privacy settings that support to shield themselves from any possible danger or damage to the internet. So, we need to know the privacy settings of social media platforms. (Pennelli, 2012). IX.
- **Anti-Virus must still be up to date: you must keep Anti-Virus Updated.** According to Fight Cyber-stalking, Trojans, worms, and electronic mail worms are popular traditions for cyberstalkers to admittance their knowledge. Everyone makes confident the Anti-Virus is updated to minimise the likelihood that one's computer will not be linked to a Trojan virus, an email virus or a worm (Pennelli 2012). This will allow us to keep the cyber harasser away from the entry.
- **Regularly check your account:** it was evident that any internet user has his or her account on social networking pages. We must update our electronic mail, weblog or internet site accounts daily, etc. By doing that, we can be in trace with our profiles on the Internet, and that reduces the risk for hacking, stalking, etc. through checking our profiles. Some women have been found not to review their account after making their profiles on social media platforms. Regrettably, once it was tested, they initiate themselves stuck (Moore 2009). internet users, particularly females, the obligation does not overlook this problem.
- **Protect moving data:** We also use public computers in internet cafes in our daily lives, etc. Note, web browsers can maintain a list of your passwords and all page visits while using the Internet on public computers. Therefore, do not hesitate to erase traces or history of your web browsers (Doyle 2012). It can jeopardize you by your little negligence.

7: Conclusion.

In India and elsewhere in the world, the emergence of cybercrime is rising. Anyone using the Internet risks becoming a target of cybercrime. Provides a myriad of resources for cybercriminals. Either to hurt innocent people. India is known to be one of the nations to follow the Information Technology Act 2000 Combating cyber-crimes; this legislation includes a wide variety of marketable and fiscal practices. Criminalities that are evident from the preamble to the IT Act, but which are pragmatic. However, there are insufficient guidelines to protect any of the offences in contrast to women Cyberspace in compliance with the IT Act. We must not interact with people whom we do not know about in order to stop cyber-crime. People who are on the other end of the machine may not be whom They are pretending to be.

We need to have our passwords safe and not have them. The hacker can exploit confidential information on the device. If something appears to be out of order or inappropriate, immediately call law enforcement. Indian female networkers are also not vulnerable to cyber-harassment or cybercrime. This existence offers the suspect an opportunity to seepage after the commission of cyber-crime. The issue will only be fixed if the victimised lady either complained back or otherwise warned the attacker against taking firm action. Police officers must be qualified to deal with and deal with cybercriminals. Workshops and workshops on cyberspace education must be arranged for this purpose. Women can also be active in this form of operation again. However people should change their views towards women and develop a sense of sharing.

References

1. Agarwal, Rohit. CYBER CRIME AGAINST WOMEN AND REGULATIONS IN INDIA. 2013. Accessed on: 24 July 2017. Available at: <http://www.tmu.ac.in/gallery/viewpointscip2013/pdf/track4/t-403.pdf>
2. Doyle, Carmel. Top tips to avoid being a cybercrime victim. 7 February 2012. Accessed on: 18 July 2017. Available at: <<http://www.siliconrepublic.com/digital-life/item/25681-top-tips-to-avoid-being-a-c>>
3. Debarati Halder, K. J. (2012). Cyber Victimization of Women and Cyber Laws in India. In K. J. Debarati Halder, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations* (pp. 113-128). Information Science Reference.
4. Empowering women against cyber-violence. 16 January 2011. Accessed on: 20 July 2014. Available at: <<http://www.theborneopost.com/2011/01/16/empowering-women-against-cyber-violence/>>.
5. Geetha, B. "Cybercrimes have grown in numbers and character. Women, the chosen victims of cybercrimes choose to remain silent about them due to outdated stereotypes — which complicates implementation of the IT Act Vulnerable in virtual space." The Tribune, Chandigarh (2011). Accessed on: 18 July 2017. Available at: <<http://www.tribuneindia.com/2011/20111107/edit.htm#6>>.
6. Halder, Debarati and K. Jaishankar. CYBER VICTIMIZATION IN INDIA. A Baseline Survey Report. Tamil Nadu: Centre for Cyber Victim Counselling, 2010: 1-22. Accessed on: 17 July 2017. Available at: <http://www.cybervictims.org/CCVCresearchreport2010.pdf>.
7. Halder, Debarati and KaruppannanJaishanKar. "Cyber Socializing and Victimization of Women." September 2009: 5-26. accessed on 17 July 2017. Available at: <<http://www.doiserbia.nb.rs/img/doi/1450-6637/2009/1450-66370903005H.pdf>>.
8. Jaishankar, K. and V. UmaSankary. Cyber Stalking: A Global Menace in the Information Super Highway. n.d. accessed on: 19 July 2017. Available at: <<http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm>>.
- 9- Jeet, S (2012) "Cybercrimes against women in India: Information Technology Act, 2000" Elixir International Journal Elixir Criminal Law 47 (2012) 8891-8895 available on [http://www.elixirpublishers.com/articles/1351168842_47%20\(2012\)%208891-8895.pdf](http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf)
- 10- Kumar, T& ,Jha, R (2012) "Cyber Crime And Their Solution" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 1 Oct 2012 Page No. 48-52 available on <http://ijecs.in/ijecsisue/wp-content/uploads/2012/12/48-52..pdf>

11: Maltais, C (2005) "Managing Cyber Crime: An Assessment of Canadian Law Enforcement Responses" available on http://cathyfmaltais.com/assets/docs/full_thesis.pdf

12: Pachauri, S. K. Women and Human Rights. New Delhi: S.B. Nangia, A P H Publishing Corporation, 2010.

13. Pennelli, Paul. Cyberstalking Awareness: Protect Yourself On-Campus and Beyond with These 7 Steps. 31 January 2012. Accessed on: 13 July 2014. Available at: <<http://blog.gradguard.com/2012/01/cyberstalking-awareness-protect-yourself-on-campus-and-beyond-with-these-7-steps/>>.
