

## Impact of cybercrime on women

Dr. Savita Madhavrao Gire

Assistant Professor, head of dep. Sociology

DJGACSC College, Vaduj

Cybercrime involves the use of computers or computer network to commit criminal activity. Cybercrime is not unique to India. As the country has experienced technological innovation in the last two decades, the use and misuse of the Internet also spread across the country. As of 2016, India is globally ranked third for “malicious activity,” whereas China and the United States have taken the first and the second place, respectively (Mallapur 2016). Also, the number of Internet users in India has reached over 330 million in 2017 and projected to grow to about 512 million in 2022 (Statista 2019). With these growing trends, the country has witnessed an increase in cybercrimes such as phishing, introducing malicious codes, identity theft, bank fraud, transmission of sexually explicit materials, cyberstalking, and cyberbullying. The chapter provides a brief description of the Indian government structure, including the legislative and judicial branches, law enforcement, legislations dealing with cybercrimes, and the nature and extent of cybercrimes. Also, the current debate about cybercrimes in the country is presented.

Information technology has widened itself over the last two decades and has become the axis of today's global and technical development. The world of internet provides every user all the required information fastest communication and sharing tool

making it the most valuable source of information. With the numerous advancement of internet, the crime using internet has also widened its roots in all directions. The cyber-crimes pose a great threat to individuals. Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. In this paper we explore the Cyber-crimes and the online security vulnerabilities against women. Cyber-crime is emerging as a challenge for national and economic security. Various issues that are discussed in this paper are: Cyber Stalking, Harassment via Email, Cyber Defamation, Morphing, and Email Spoofing against women.

Cyber-crimes use information technology and the internet as the primary means for commission of illegal activities, which are prohibited and punishable by criminal law of the land. While cyber-crimes may be committed against persons, property and the government, this paper focusses on cyber-crimes against women. The more common and frequently reported forms of cyber-crimes against women include cyber stalking, cyber pornography, circulating images / video clips of women engaged in intimate acts, morphing, sending obscene / defamatory / annoying messages, online trolling / bullying / blackmailing / threat or intimidation, and email spoofing and impersonation. Various forms of cyber-crimes are experienced by Indian women who use the internet in the contemporary context. Neither the IPC provisions nor the provisions of the IT Act fully reflect the ground realities of women's experiences. In many situations, such as morphing, email spoofing and trolling, IPC provisions are applied by extrapolation and interpretation for the want of more specific provisions of law. Although the IT Act contains a chapter on

offences, including computer-related offences, the provisions deal mainly with economic and financial issues; there are no specific provisions on cyber-crimes against women even though they are rampant and are widely reported. The first step towards providing legal remedies for women is to ensure that the online experience of harassment / threat / intimidation / violence caused to women is accurately translated into the written law through amendments to the two major statutes.

**Statement of the Problem** - Cybercrime is the alarming concern which has sprung in recent times and perhaps it is the most complicated problem in the cyber world that requires immediate attention and promising strategies from the society, government, families and individuals. Limited authenticated and reliable statistics on the nature of crime and the monetary loss of the victims are available for reference, almost of these crimes are never brought into record. A specific and effective study on the occurrence and avoidance of such disturbing cybercrimes would be a good area of research today. Over the last two decades the usage of internet has taken a giant leap. However, researchers have begun to study such cases and problems only in the later years. The purpose of this study deals the nature and kinds of cybercrimes against women and girls, how women can be protected from these crime and what steps could be taken to prevent them.

**Literature Review** – Nidhi Arya, (2019), has explained the terms of cyber space, cybercrimes etc. Through the study author has discussed on the implementation on enactment of cyber law in India. Author has also focused on the various types of cybercrimes and its functions. Through the study author has also

discussed on the problems faced by the police for investigation on cybercriminals. Through the study author has discussed on the role of judiciary in expanding cybercrime jurisprudence. Sarojani Chiluvuri, (2017), has also focused on the types of cyber savagery against women and girls in India. Author has also focused on the impact of cybercrimes against women in terms of social and psychological conditions. Through the study author has discussed on the provisions of IT Act, 2000 relating to cybercrime and offences against women in India and focused on the loopholes of this Act. Through the study author has suggested some preventive measures to overcome the social evil of cybercrime. Sunil Kumar, (2020), has analysed the cases pertaining to cybercrimes against women in Delhi. Author has further discussed on the various reasons for cybercrimes and also discussed on how women can abduct themselves from cybercrimes cases and if convicted what they need to do. Through the study author has focused on the cybercrimes rate in India and Delhi. In the opinion of author, there should be more stricter laws for the Internet services providers for ensuring the safety and securities of women and minor girls.

### **Objectives of study**

1. To assess the awareness about cybercrime among women
2. To investigate the nature of cybercrime among women

Scope of the study -The scope of the present study is confined to the study of impacts of cybercrimes against women and its impacts on their family and social life. Therefore, this study does not focus on the other types of cybercrimes. From the study

purpose specified sample unit has been selected, that is the women, victimised in cybercrimes committed against them.

Data collection- Required information (data) has been collected through primary and secondary sources.

### Laws against Cybercrime in India

Ever since the introduction of cyber laws in India, the Information Technology Act (IT Act) 2000 covers different types of crimes under cyber law in India. The following types of cybercrimes are covered under the IT Act 2000.

- **Identity theft** – Identity theft is defined as theft of personnel information of an individual to avail financial services or steal the financial assets themselves.
- **Cyberterrorism** – Cyberterrorism is committed with the purpose of causing grievous harm or extortion of any kind subjected towards a person, groups of individuals, or governments.
- **Cyberbullying** – Cyberbullying is the act of intimidating, harassment, defaming, or any other form of mental degradation through the use of electronic means or modes such as social media.
- **Hacking** – Access of information through fraudulent or unethical means is known as hacking. This is the most common form of cybercrime known to the general public.
- **Defamation** – While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.

- **Trade Secrets** – Internet organization spends a lot of their time and money in developing software, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offense.
- **Freedom of Speech** – When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.
- **Harassment and Stalking** – Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offense.

IT Act, 2000 went through amendments under the Indian penal code in the year 2008. These were made in light of the laws on cybercrime – IT Act, 2000 by way of the IT Act, 2008. They were enforced at the beginning of 2009 to strengthen the cybersecurity laws.

In societal life, we often encounter changes in all aspects of life, including changes in the community itself, because there is essentially no static society. There are always changes in society dynamically. Either the changes build up in the sense of positive impact in the future for the community or instead bring a bad impact to the community. The change is a technological innovation. Technological advances are also advancing information. Information can be obtained from friends, family, print media and electronic media. Especially in today's modern era, many people are already using new media that is Internet media [1]. The use of the Internet is not a special thing or

particular for certain circles, both in terms of profession, community, education and age. Almost all groups of people already know and are familiar with the Internet. Along with the development of time and the modernization of the Internet becomes a necessity and human activity as community members. In addition to being a professional prosecution, professional development, scientific development, news, and entertainment, Internet is also an alternative way for someone to interact as a social creature. Internet presence makes it easy for people to make information and data that is not necessarily found directly in the print media that can be encountered daily. Especially because the obstacles are way and costs are not small. there can be internet cafes that scattered along the roadside. In addition, there are many public places, educational institutions, cafes, malls, and recreation venues that offer hotspot or Wi-Fi services to people who have laptops or notebooks. Besides, there are many types of mobile phones equipped with Internet applications. Activities based on Internet technology, is now no longer a new thing in the information society. The Internet has even been used by children of preschool age, parents, businessmen, agencies, employees to housewives The research shows that only few users are not aware about cybercrime. There are ample number of tools and resources available to sort such matters of concerns. Adopting few preventive measures and best practices, we can surely keep cybercrime at bay. To implement more effective prevention strategies, it is mandatory that educators, parents, law enforcement, and legislators understand the root cause of the occurrence of such cybercrimes. Schools and colleges should regularly educate both students and parents on safe surfing, through workshops and seminars. Awareness of cybercrime

should be a part of regular course work in educational institutions. The free internet facilities provided to educational institutions should be carefully monitored and kept secure. Cyber cells and cyber court assigned to deal such proceedings should be increased in number. Productive tie ups between IT companies and law enforcement authorities may help in tracking and penalizing individuals who indulge in such crimes.

## References

- 1 Santosh Rout (2008), Network Interferences, Available at: <http://www.santoshraut.com/forensic/cybercrime.htm>, Visited: 28/01/2012  
By Jessica Stanicon (2009), Available at: <http://www.dynamicbusiness.com/articles/articles-news/one-infive-victims-of-cybercrime3907.html>, Visited: 28/01/2012.
- 2 Rasun Sonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: <http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html>, Visited: 10/31/09
- 3 India emerging as major cyber crime centre (2009), Available at: <http://wegathernews.com/203/indiaemerging-as-major-cyber-crime-centre/>, Visited: 10/31/09
- 4 TI Contents (2009), India: A major hub for cybercrime, Available at: <http://business.rediff.com/slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm>, Visited: 28/01/2012.
5. hobhana Jeet, (2012), “Cybercrimes against women in India”, Information Technology Act, 2000”. Elixir International Journal,

No 47. Nidhi Agarwal, (2014, “Cybercrimes against women”, GJRIM, No 4. N. Arya, (2019), “Cybercrimes scenario in India and Judicial Response”, International Journal of Trend in scientific Research and Development Vol.3, No Scholarly Research Journal for Humanity Science & English Language, Online ISSN 2348-3083, SJ IMPACT FACTOR 2019: 6.251, www.srjis.com PEER REVIEWED & REFEREED JOURNAL, AUG-SEPT, 2020, VOL- 8/41 Copyright © 2020, Scholarly Research Journal for Humanity Science & English Language IMPACT OF CYBERCRIME ON WOMEN VICTIMS IN PUNE CITY Raju Gaikwad<sup>1</sup> & S. I. Kumbhar<sup>2</sup> , Ph. D