Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July-December 2023 4(2), 3984–3988

INTERNATIONAL SCENARIO OF CYBERCRIME AGAINST WOMEN IT'S EVOLUTION AND EFFECTS ON PERSONAL LIFE

Abhilasha Vaishnav [1], Prof. Dr. Beena Dewan [2]

[1] Ph.D Scholar (Law & Governance), Jayoti Vidyapeeth Women's University
[2] Faculty of law & Governance, Jayoti Vidyapeeth Women's University

DOI
10.29121/shodhkosh.v4.i2.2023.4513

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Over the recent years, Cyber-Crime has become one of the major concerns of the world. However, India deserves special focus in this context as it has one of the highest rates of cyber-crime in the world. Indian women are the most likely demographic of the country who are likely to affected by these types of crimes. It describes the origin of cyber-crimes, and the way women are most likely to be the victims of these types of crimes. Since, special focus has been put on India, the cyber-laws, and their loopholes have also been addressed. In addition to that, also addresses the gaps that exist between legal actions, and advancements in technology. Lastly, several cases related to cyber-crimes, and the laws that were implemented during those cases have also been discussed. Discussion is also made about relationship between women, and cyber-crimes in an international perspective. Several reports and articles have elucidated the fact that the condition of women affected by cyber-crimes is very similar to that of women in India. This situation has taken negative turn ever since the global lockdown. This case is even worst in the case of countries located in the Middle East, and other developing countries. In the significance of overseas law and cyber-crime related law is been discussed. The impact of these laws in mentioning the security of women is also discussed.

1. INTRODUCTION

International Scenario

Cybercrime is considered as a growing concern over the years. Number of cybercrimes has increased by 18.4% from 2019 to 2021. Report of NCRB (National Crime Records Bureau) shows that number of cybercrimes against women has increased by 28%. Primarily, cyber blackmail, threatening, posting various material of obscene sexual things, cyber pornography, stalking, bullying, fake profiles are included in cybercrime. Increasing rate of spread of technology, internet led to emergence of cybercrime.[1] Research from the World health organisation shows that one in three women are

experiencing cyber crime in their life. In this technological era, it shows that one in ten women have experienced cyber violence. This is a critical and challenging situation for women. Cybercrime prevention against women and children (CCPWC) is a scheme where effective measures are taken to handle and control cybercrimes against women and children in India. This scheme allows victims to file complaints against cybercrime.

In time of Covid-19 more girls and women were victims of cybercrime. There are many cases of cybercrime under VAWG which highlight Arab region. In addition to this, concerning issues are raising about Facebook cloning. Cyber-crime against women has increased due to emergence of information technology and internet access everywhere. There are several reasons for growth of cybercrimes against women which are nature of internet which has no boundary or limitation, various vulnerable targets, cases of cyber-crime that are not reported or complained about properly due to fear, societal pressure, hesitation and so on.

Enhancement and Enactment of overseas laws of cybercrime

International laws face challenges about international cybercrimes. It creates challenges for framework of domestic and international laws and regulations. Laws which are existing in international laws and regulations are not well fitted for cybercrimes. Changing nature of cyber bullying and harassment. Advantages of improper judgment and punishment led to increased cybercrimes. Cybercrime is often associated with various forms of cyber-attack like Trojan, Malware, Ransomware, phishing and so on.[2] In 1997, G8 was made of eightcountries including the U.S, UK, Russia, France, Italy, Japan, Germany and Canada. Includes various actions which can control cyber-attacks and crimes. 156 countries develop cybercrime laws and patterns are different from one country to another. Europe has highest number of adoption rates which is 91 % and Africa has lowest number of adoption rates.

Cybercrime Prevention Act, 2012 which is targeted at preventing various cybercrimes which include privacy violation, violation of confidentiality and information about cyber-criminal activities. The Indecent representation of women prohibition act which regulate and prohibit various representation of women by various media and publication. It also includes contents which are in electric form, various portrayal of women from various web. Various initiatives are taken from Governments which enhance cyber security. There various cyber security laws and regulations which are protection of harassment act 1997. It is an important law related to cyber bullying. IPC section 292 deals with pornography which deals with transfer, distribution and sale of obscene material is punishable and can be imprisoned up to 2 years and a fine of Rs. 2000 or both. Section 67 of IT act, 2000 which include circulation and distribution of obscene material can be imprisoned for 3 years and fine up to 500 Rs.

Legal Treatment of Cybercrimes Against Women in USA

There are various laws and regulations in USA to remove cybercrimes against women. In section 2701 of chapter 121, USC 18 (part 1) which is applied to such cases of cybercrime and bullying against women. It includes such offenses like attacks on computer networks, unauthorized access, distribution of obscene images of women on the internet. Violations of this law include hacking a female victim's picture, humiliating her in front of a large audience and so on. Thai law punished these accused by imprisonment of 5 to 10 years and with fine. Rapid and increasing growth of internet and increasing cybercrimes are evidenced in the USA. In statistics of WHOA 2000, among 353 respondents 83% of victims are females and harassers are about 68% male in which only 27% harassers are female. In these statistics, 39.5% of cyber-attacks are done by email, 17.5 % from message boards and 15.5% from chat rooms. In 2021, Phishing and related cybercrime is most commonly considered cybercrime in USA. In this almost 324 individuals have affected.

Even though there are various legal provisions about cybercrimes against women there is also some lack of provisions for this. Hacking is regulated by computer fraud and abuse act which is under this act. In case of information of women are stored in personal computer website, network profile which are often targeted by perpetrators and online harassers hacking of email id. Her yahoo account was breached and private emails were posted online by a college student. Former Alaska governor Sahara Palin, US vice presidential nominee, took the paradigm of victimization of women which is based on the above issue.

Legal Treatment of Cybercrime Against Women in UK

In UK there is a growing concern about cybercrime against women. Five year imprisonment and ultimate fine is UK's rule applied against cybercrime. Cybercrime against women include cyber blackmail, cyber pornography, publishing

various obscene material, stalking, defamation and creation of fake profiles. In UK, cyber criminals which include exploitation of human or security vulnerabilities to steal information and password and unethical hacking. In section 43, cyber criminals will be punishable with imprisonment of three years and with a fine of five lakh rupees or both. In section 66, any person who is dishonestly and fraudulently which is referred in section 43 can be imprisoned for three years and with a fine of five lakh rupees.[3] There are some advantages in UK in which anyvictims can file a complaint against cybercrime and report online by calling 101. Cyber flashing is introduced as a new cybercrime in UK.

In the World Health Organization, it shows that one in three women have faced violence in her lifetime. Growing phenomena of technology and internet led activity of cybercrime. It has been estimated by WHO that one in ten women have experienced cyberbullying under age of 15. VAWG is not properly conceptualized against EU level. EIGE has conducted desk research which helps to understand better about harmful cyber VAWG. As per global report, China, United states and India is a leading country in cybercrime against women. According to these reports, These countries have faced the most critical cybercrime.[4] Morphing is considered as most widely used mischievous which is regarded in women victimization in cybercrime. It includes unauthorized access to personal pictures of females. This activity is associated with hacking and modification of various web accesses. Hacking social media and email accounts is most common cybercrime in UK. There are also some lacks of laws to control cybercrime against women. Various laws and regulations have been enacted to reduce cybercrimes against women and provide a framework about various criminal offenses and provisions for cybercrime.

Cyber Privacy and Related Offences against Women

Canadian women face data infringement in online platforms which intrudes their private space to a large extent. Therefore, they undergo incidents like threatening messages, blackmailing emails and modification of their own pictures which bring upon a state of utter shame. This /are regulated through the Criminal Code Act, 1993 of Canada.

Even at times women's accounts get hacked online by hackers. This is regulated in the context of Canadian women society through aforesaid provision under the Section 342.1. Therefore, all hacking related activities are covered under its legal action. Not allowing the original owner in accessing their private data is considered to be a punishable act for the alleged person who is found indulged in such mischievous activities of abrupt modification of the owner's original content. This is covered under Section 430 (1.1) convict gets penalized for mastering with personal data of respective owners.

Offensive Communication Against Women

Problem of online hate speech is more than prominent in the Canadian scenario. Therefore, such contexts of spreading hatred through speech are viewed from two angles. Firstly, "Cyber Defamatory libel" which is targeted by youth and adults to other youths and adults. Secondly, "Cyber Hate Propaganda" which is generally targeted by adults to either an individual or a community based on caste, creed, race and religion. These two perspectives are regarded as sources of creating disharmony in an individual's mind or within a community.

"Cyber Defamatory libel" is considered to be a criminal offence under "Part VIII of the Canadian Criminal Code of 1993". Moreover, Section 298 addresses such communicative hate speeches which either insult or defame any individual or a community. Thus, this legislation helps in mitigating the spread of hatred which might provoke national turmoil and disharmony. In this regard, women individuals are also protected from any sort of hate speech that is offered to them by cyber attackers on online platforms extensively. It is, however, not so effective at times for women's security from hate speeches or offensive content.

"Cyber Hate Propaganda" as dealt with in "Part VIII, Section 319 of Criminal Code of Canada '' which helps in safeguarding women from hate messages and comments that instigate their social defamation procedure. "Section 318", thus establishes the fact that any person of Canada cannot be distinguished through any discrimination speech irrespective of colour, race, ethnic origin and sexual orientation. Moreover, "Section 13 of Canadian Human Rights Act" is implemented by the government to prohibit any communication by means of a telecommunication undertaking including the Internet facilities, regarding sending offensive messages which reflect utter hatred or obscenity.

Responsibilities of the ISPs

Canadian Human Rights Act (CHRA) regulates hate speeches extensively which has already been discussed earlier. Section 13 of CHRA also in its subsection 3 exempts ISPs (Internet Service Providers) from criminal liability. For instance, as per the Canadian Criminal Code, the proprietor of any newspaper where defamatory libel has been published with his knowledge may be pulled in for sharing the responsibility as offender with that of the original writer of the defaming message. It is noted that in case of a female victim, reports of defamation or hate propaganda on the internet to the police, it should be judged from the angle of "discriminatory practice" as under Section 13 of the CHRA and ISPs may be exempted in that manner. However, the case should also be read with the provisions of the "Criminal Code under Section 301 in case of defamatory libel" and "Section 319 in case of hate propaganda", to treat them as a means of criminal offence.

Safeguarding Women in India: Strategies for Preventing Cybercrime

The various dimensions of cybercrime are such that in existence of dark web along with deep web, anyone cannot able to ascertain the point extent of this matter. Furthermore, this has established a worry and a sorry for some state of affairs. Therefore, cyberspace is considered to be a vital gift provided due to globalisation and also for significant advancement of technology and innovation[5]. Furthermore, this has become one of curses in this 21st century as there is a misuse of it, which leads to an adverse effect on people of India and it is reported those women mainly get affected due to it. Furthermore, it is reported that due to killing effect of cybercrime, the rate of it gets increased among women in this country by 6.23% from 11590 cases in 2015 to 12,316 cases in 2016 as reported by "National Crime Records Bureau".

Moreover, it is reported that in India, majority of cases are under cyber crimes and it is also analysed that use case is prim daily generation from Uttar Pradesh, which accounts for approximately 2630 cases which is almost 21%. Other cases are accounted for from Maharashtra, which is 20% and whereas in Karnataka, cases like this are generating by 9% in 2016[6]. From here it can be seen how cyber crime impacted professional life of many people and it is also reported that some prestigious places in India are highly accountable for it, which is a downfall and shameless factor for country. Moreover, in 2016 about 49% of cases of cyber-crime cases is accountable due to illegal work which is 9% and some other factors that are related to insulting the modesty of country's women with almost 6% which is 680 cases.

Therefore, tackling formulation in a country for cybercrime is considered to be as "Information Technology Act, 2000" and this is also considered to be a kind of half-backed law. Moreover, priority was primarily given in order to protect e-commerce section along with communications and for tit communications which are cyber-socializing therefore, remain untouchable with not regarding women who get victimised due to cybercrime in India[7]. There are cases regarding cyber crimes such as online threats of blackmailing and molesting along with hacking some important data from authentic websites that create an adverse impact on women in country. In addition, online threat is also linked with derogatory type of messages and creating social media pages in order to defame someone for this freedom has been taken from women in country due to cybercrime which also increases cases of suicide among them due to depression, which creates among them (Bhat *et al.* 2022). However, in India, this kind of defamation and online threat is strictly prohibited and punishable under the law which creates several offences that creates mental violence. It is reported that cybercrime primarily affects many women in a country that is subjected to emotional harassment and mental. Majority of women are gradually becoming distressed due to it and remain humiliated due to this crime and it needed to get strictly addressed along with resolving it.

Furthermore, violence and cyber crime evolve from using internet and making use of computer technology, which gets access to personal information of women in country along with usage of internet to mentally exploit women. It is understood that women are generally soft and reason why they get often targeted also they trust easily anyone, which is

the reason that they get unaware of consequences[8]. Moreover, cyber chrome gets increased as it is not easy to identify the person behind it and is often seldom reported. Therefore, this is also not easy to monition by following all kinds of traditional approaches as it is earlier said that person who involves in this type of crime is not easy to get identify and is a reason such cases are increasing at a rapid rate. Additionally, it affects a majority of women, which is primarily subject to harassment in an emotional manner and most of them get depressed due to it, which is required to get quickie resolved.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Choirunnisa, Sutiani. "Legal Protection Against Women Victims of Sexual Harassment Through Social Media (Cyberporn)." *The Indonesian Journal of International Clinical Legal Education* 3.3 (2021): 367-380.

Sangwan, Pooja. "A Critical Study of the Violation of Women's Right in India with Special Reference to Cyber Crime." *IME Journal* 13.2 (2019): 148-155.

Al-Nasrawi, Sukaina. "Combating cyber violence against women and girls: an overview of the legislative and policy reforms in the Arab region." *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (2021): 493-512.

Bhongale, Dr, and Jay Kumar. "Crime against women in cyber world." *Crime against Women in Cyber World (August 12, 2021)* (2021).

Pew Research Centre, 2022, HOW INDIANS VIEW GENDER ROLES IN FAMILIES AND SOCIETY. Accessed on: 29th Sept, 2022. Accessed from: https://www.pewresearch.org/religion/2022/03/02/views-on-womens-place-in-society/#:~:text=About%20a%20quarter%20of%20Indians,before%20the%202019%2D2020%20survey.

Abukari, A.M. and Bankas, E.K., 2020. Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11(4), pp.1401-1407.

Achsin, M.Z., Seniwati, R., Triyanto, M.Y.S.J., Ninggara, N.A., Rafifah, S. and Gularso, S.N., 2020, May. The Role of Non-Governmental Organization in Preventing Violent Extremism in Indonesia: The Case of Wahid Foundation. In B-SPACE 2019: Proceedings of the First Brawijaya International Conference on Social and Political Sciences, BSPACE, 26-28 November, 2019, Malang, East Java, Indonesia (p. 125). European Alliance for Innovation.

M. and Nurse, J.R., 2019. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security.