Law Journals
A Unique Issue of Legal Knowledge

National Journal of Cyber Security Law

Volume 3, Issue 1
www.stmjournals.com

Women Safety in Digital World

Shreya Kalyani,[1,*], *Shambhavi*[2]
[1,2]Student, Chanakya National Law University, Patna, Bihar, India

Abstract

As the world embraces a digital life where we are able to connect to anyone in any part of the world. Internet has become our second life and mobile phones an extension of our personalities. On the other hand, security in the digital world is a matter of great concern because of cybercrimes and other mischievous activities related to digital environment. Lack of technical awareness and proper imposition of law governing cybercrimes worsen the victim's plight. So far, it is observed that large number of cybercrimes related complains are not being registered to the concerned authorities and also there is lack of proper follow up in these cases. Even the latest technologies and networking sites needs high level of security. Workplaces of women are more prone to cyber security hazard due to the nature of our modern digitally dependent work environment. Cybercrimes related to women dignity are also not being reported due to social stigma. The paper draws together existing data on the dimension of violence and ugly side of the digital world of women in particular, that prevailed worldwide including reviews and literature as case studies of the mental consequences of such harassment. It also explores important steps that women should follow for safe and secure working in social digital world. Besides so many measures the security in the digital world is the most important concern every user in the digital life has. To assist policymakers in addressing this issue, the paper explores insertions in primary prevention, cyber ethics, cyber care response, programs to assist victims. It argues that any strategy to combat mental and physical harassment must attack the root causes of the problem in addition to treating its symptoms. This means challenging the old security measures and opening all domains of new encryption trends for security purpose. Against every evolving cyber threat, the law makers must enact effective laws which provides for appointing skilled graduates to deal with different ways of securing and relieving women from the terror of crimes in digital world.

Keywords: *Digital, cybercrimes, mobile phones, policymakers, harassment, women dignity, security, encryption, terror, cyber ethics*

****Author for Correspondence*** E-mail: shreya.kalyani10@gmail.com

INTRODUCTION

Women tend to suffer all forms of violence in this male dominant society and nowadays prevalent and the most often mishap is that of cyber violence which has shown a rising trend. Internet has opened up new opportunities for more gender equality and participation. There is a huge gender gap in the workplaces and the figure could shoot up even further, if the safety of women is not ensured in such workplaces. Although the digital world may exist only in intangible form, it affects the real environment. The fast evolution of digital world has helped the whole world to access information at anytime from anywhere, but it is also accompanied by the vulnerabilities of society to cybercrimes. With the help of technology, people also tend to remain more updated about the current events via online media sources and to coordinate location within a few seconds via GPS etc. However, technology also contributes in ensuring the women safety to some extent via wearable equipment and SMS-based app services. On the other hand, it also acts as a weapon for the abusers to harass and blackmail women through cyber means. The major role of the state is to promote safe internet use which does not attack public especially the women from getting fooled and black mailed. These forms of mala fide intended activities also threaten the security of people thereby, affecting the social harmony. Many cases remain unreported and most of them even

which are reported go unresolved which is the reason that true enormity of cybercrime and its demographic statistics could not be proportionately ascertained. There remains a lack of cooperation with the foreign based websites which becomes one of the barriers in resolving the cybercrime related cases. The security is the major concern that every internet user has nowadays because now it is not just limited to securing passwords, contact details, photographs from the stranger.

CRIMES IN THE DIGITAL WORLD

Digitization though offers a lot of opportunities to the women around world to showcase their talent and present their ideas where the world can know and appreciate their efforts but these advantages come with some dangers posed to women in digital world. Digital world in practical life does not appears to be safe for women because of the breach of privacy, hacking the personal data such as medical records, sexual preferences, financial status and revealing them to the unauthorized strangers. If equality in digital sphere is not maintained then it will be the sheer insult of talent, vision, resources and wealth. The lack of diversity, particularly women in the various fields has an impact on innovation and growth [1]. In recent times there have been gamut of news reports about targeting women through digital media where their safety is being damaged and compromised. For instance, certain pictures of an Udaipur girl were taken from her social media account and was circulated on the internet after deforming it. In addition to this incident there are a lot more incidents which take place on a regular basis many of them also remain unreported as a result of which no action is taken and the perpetrators do not come to light. Online harassment can involve sexual harassment which is unwanted contact of a personal nature, or the other conduct based on sex affecting dignity of women at work. It may happen in various ways. One form may include sending unwanted, abusive, threatening or obscene e-mails [2]. Another form may include electronic sabotage or spamming where the victim is sent hundreds of junk mails accompanied by computer viruses. The third common form arises in live Internet relay chat sessions, message boards or news group by way of instant messages [3].

Cybercrime is prevalent in the digital world which relates to the vandalizing and violation of the network system, it is commonly used to mean crimes and breaches in relation to computers which are not connected to the internet [4]. It may consist of freeing of a virus into the network, the defacing of computer data or it may also be an unauthorized access into the information stored in the computer [5]. Cybercrimes have particularly captured the attention of the public and media specially in India where the situation is more alarming. Indian organizations have reported 53,000 security incidents in 2017 alone as revealed by CERT-In. Main issues which are revolving around includes mobile text messages, intimate photos and video blackmail, lack of consent and email accounts control. There are cybercrimes which have been provided in IT Act such as tampering with computer source documents, hacking with computer system, publication of information which is obscene in electronic form, to secure access to a protected system without any authorization and breach of confidentiality and privacy. Some of the other cybercrimes have been classified as follows:

Cyber Defamation

Which refers to publication without any lawful excuse which is done to injure the reputation of another by exposing him to hatred or ridicule. This can be done through World Wide Web, E-mails and social networking sites like Facebook, Twitter. Though it is a new concept but the definition of defamation is applicable to cyber defamation also as it involves defamation of a person through other means i.e. electronic means which is new and virtual. The harm caused due to cyber defamation on a website is severe and extensive which is exposed to the whole world. In the case of SMC Pneumatics Pvt. Ltd. V. Jogesh Kwatra, employee of the plaintiff company defamed its firm by sending vulgar and offensive e-mails to different subsidiaries all over the world with the intention to defame the reputation of the said firm. Consequently, the offender was

restrained from sending those derogatory and abusive e-mails by the court.

Cyber Bullying

Can be defined as the use of electronic communication to bully a person, typically by sending messages of an intimidating and threatening nature [6]. It includes causing deep harassment, embarrassment and public insult using electronic means like cell phone, computers, SMS, social media. Till date there is no specific legislation for cyber bullying although it has been partially included in some of the provisions of IT Act, such as section 67 of the act which penalizes the publishing of information which might be obscene, through electronic means. Cyber bullying is more as compared to the traditional forms of bullying since it involves social media which can reach out to the close friends and acquaintances resulting into severe embarrassments and shames. Girls tend to suffer more on the digital platform as compared to men some of which includes: sending or posting vulgar messages online, threatening to commit acts of violence, hacking person's account.

Cyber Stalking

Is where the perpetrator is accused of meticulously following the places of the user's visit through online means. Stalking exists from a long time even before the time when internet did not come into existence. This was experienced by women mostly while they were out of their house either returning from a school, college or workplace for the purpose of making unwarranted advances towards the women. And when they refuse to such advances, they follow the same practice as a way to harass, intimidate or defame them. Since the perpetrator due to electronic means has an advantage of no tangible evidence due to which he remains unidentified and cannot be traced easily. It has been observed through the figures that most of the time, inexperienced web users, emotionally weak persons and young girls are the victims which leaves potentially devastating effect on the minds of victim. Cyberstalking has been made an offence under Indian Penal Code, 1860 by adding Section 354-D by virtue of which on first conviction there is a punishment of simple or rigorous imprisonment up to three years with fine and on second conviction it is up to some years. India's first conviction for cyber stalking was done after 15 years of the cyber laws coming into existence because IPC sections did not cover internet crimes as a result of which most of the cases of cyber stalking went unpunished. Under section 354-C, a person who takes pictures of a woman, or watches her where she expects privacy or when she is indulged in some private activity has been directed to be penalized.

In 2001, India's first cyberstalking case was reported which caused the Indian Government to think of need of amendment of laws regarding cybercrime and protection of victims. The offender was stalking an Indian lady by illegally chatting on the website using her name and also used obscene and offensive language and distributed her phone number, residence and other personal details. It resulted into her getting obscene calls. The case was registered under Section 509 of IPC for outraging victim's modesty. However, this section refers to the act, gestures and words and the same things done over the internet have no mention therefore, the offender was arrested and later released on bail. This induced the government to bring some necessary amendments regarding those crimes.

Yet another crime prevalent in the internet world is **cybersquatting** which is referred as registering, trafficking in or making misuse of a domain name intending to receive dividends from the goodwill of another trade mark or business house [7].

Hacking

Is another category of cybercrime which is the most exasperating of all, committed via the internet resulting into serious security breaches which are individual privacy concerns and national security concerns. It is referred to as unlawful access to a computer system which includes breaking a password protected website, evading password protection on a computer system.

According to the reports of India's Computer Emergency Response Team 44679, 49455,

50362 cyber security incidents are reported in the year 2014, 2015 and 2016 respectively [8]. Cybercrime perpetrators are not restricted by any geographical boundaries. There are other cyber-attacks which have been prevalent these days such as virus and worm attacks. Emails play a very significant role in the especially in the workplaces to build an effective relationship formally with all the prospects, leads and the customers any time according to their convenience and is a fast as well as reliable form of communication. However, this has not remained that reliable because of email spoofing, spamming, and bombing which involves sending of malicious codes through the emails, and breach of privacy and confidentiality. There are some other crimes as well which have not been included in the IT Act. They are as follows:

Email Bombing

It is sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing the system or a network.

Data Diddling

Involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

Web Jacking

The owner loses control over his system and the word has been taken from hijacking.

Keystroke Logging

It involves capturing and recording the keystrokes of a user which is used as a tool and used to extract passwords and encryption keys and thus over-ride security measures [9].

Legal Provisions

The first step taken by the government of India with regard to cyber security was National Cyber Security Policy, 2013 which aims at protecting as well as safeguarding the personal information from cyber-attacks, build capabilities to respond to such attacks and minimize damages through the processes and technology. In 2014, the position of National Cyber Security Coordinator and in 2016 the Chief Information Security Officer was established. Other agencies which deal with cybercrimes in India are National Technical Research Organization, National Intelligence Grid and National Information Board. India has also signed various bilateral agreements such as Russia, US also including Indo-Israel cyber framework with Israel signed by the Prime Minister of India. The Information Technology Act deals with various cybercrimes in Chapter IX and XI

Cybercrime has not been defined in the IT Act, 2000 however, after 2008 amendment some separate offences committed via electronic media have been included. Section 66-A of Information Technology (Amendment) Act, 2008 deals with the offence of cyberbullying to some extent. It prescribes punishment of three years and fine, for those sending offensive messages through communication service etc. in the case of women victim this provision is also supplemented with relevant provisions of IPC, 1860. Since the nature of evidence is volatile and vague in the digital world there may be arrests which are unjustified so to avoid any misuse and ensure the effective implementation of this provision, it has been issued that the arrests may me done only after taking approval from an officer of the Rank of Inspector General of Police. Section 66A of the IT Act attempts to cope with the problems where victims are induced by the alleged millionaires to share their credit information in return for some shares. Section 72A of the IT Act imposes penalty who have obtained and disclosed personal information of a person without his consent with an intent to cause wrongful gain and wrongful loss. There are other provisions also which penalize cybercrimes such as Section 66E for violating privacy, 66F for cyber terrorism, 67 for publishing obscene material in via electronic means and Section 75 for offences committed outside India.

India has no specific data protection authority, and thus matters are adjudicated by authorities empowered under the IT Act. The IT Act provides for the appointment of an adjudicating officer, who will oversee matters related to the contravention of the IT Act or its

Law Journals

rules where the claim for injury or damages does not exceed Rs.50 million. If the claim exceeds Rs.50 million, the adjudicating authority will be the civil court. The secretary to the Ministry of Information Technology in each state government has been appointed as the adjudicating officer [10].

In the case of State of Tamil Nadu V. Suhas Katti, the perpetrator was convicted under IT Act, 2000 of posting of obscene, defamatory message about a divorcee woman and was also forwarded to her, which resulted into random annoying phone calls to her. Police traced the offender and arrested him who later disclosed that he harassed her over the internet due to being rejected by her for marriage. The case was files under section 67 of the IT Act, 469 and 509 of IPC. The court finally convicted the accused and sentenced him of rigorous imprisonment for four years and one simple imprisonment under both IT Act and IPC. He was also penalized with a fine of Rs. 5000.

Technology has in certain ways also helped women by developing certain supports to help women. In addition to the legislation there are many other apps that have been evolved in the digital world to ensure safety of women. These have been developed to enable women to feel safe in the streets and continue with their daily life instead of being confined in their homes. First, m-indicator, an app for the women travelling alone in the railways. This app features a manual SMS emergency tool and sends details of the user's location on the train and calls upon the assistance of Mumbai's Railway Protection Force. Second, Safeti pin through which the user can send her location with friends and family in case she is feeling unsafe and is also accompanied by an emergency alarm. Thirdly, there is Safe City which allows the women to share their experiences which contributes as a great help for others to make their streets safer while travelling through reporting the negative interactions. This app also uses its collected data to petition for improvements of the locality and actions to be taken for making it safer than before.

Whom to Approach:

In case of any cybercrime, one should immediately approach the Law Enforcement Agency which is the Cyber Crime Bench or any nearest Police Station in the respective area and lodge FIR for the same. The Enforcement Agency then contacts to Indian Computer Response Team, established under the Information Technology (Amendment) Act, 2008, for the technical study and inspection of the reported crime. In case the perpetrator or the computer system is located outside India, it would be deemed for the purpose of prosecution to be located in India [11].

Reasons for Increase of Cyber Crime

One of the major barriers to addressing such issues is the lack of an appropriate and special legislation in such matters. The capacity of computers to store large data in a small space which can be accessed very easily through implanting the computer system with logic bombs. While protecting the computer system the users might be negligent, this gives the cybercriminal to grab the opportunity to gain unauthorized access and control over the computer system, and data which is stored on the computers can be easily destroyed becomes a great hindrance to the investigation agency and may cause loss of evidence. Women are mostly unaware about privacy policies and safety tips for using social media sites and are comparatively less proficient in using technology. Cyber laws have not been formulated properly and the procedure for registering a complaint is not known by woman [12]. This plays the major role behind numerous cyber cases going unreported in spite of special provisions being made in the system regarding cyberspace.

Loopholes in the System

The Act has not dealt with offences such as Cyber stalking cyber harassment, cyber nuisance, and cyber defamation which are on the rise recently. However, the IT Act 2000 read with the Indian Penal Code 1860 is capable of dealing with these kinds offences to some extent. The term obscenity is not defined clearly anywhere. The obscene materials are

disseminated without any universal agreement of its terminology. Different nations have different acceptations according to their morals. For example, in Scandivia, naked pictures are not considered offensive. On the other hand, Saudi Arabia has strict orthodox Islamic principles and nudity can also be considered unlawful. In India S.67 and 67A are the provisions dealing with obscenity and there is a punishment for transmitting obscene materials. But a major thing to be noted is that the term 'obscene' only deals with the material which is likely to corrupt the minds who are open to such influences. Even IPC section 292(1) does not make knowledge of obscenity an ingredient of the offence. Thus, to escape criminal charges, one has to prove his lack of knowledge of publication or transmission of obscene information in electronic form. Though, transmission of obscene materials may be illegal but mere possession, browsing or surfing of such contents is not illegal [13]. So it is quite evident that the term itself does not have its universal identification and due to its weak influence the conviction is less and the term is less deterrent. Also due to lack of awareness many cases go unreported. Internet documents are copied and transmitted through various intermediaries and hence, it is difficult to identify them as well as the hosts. Internet itself is a jurisdiction which has turned into a privacy intruder. Physical world intermediaries are conscious actors in the transaction, whereas internet intermediaries are often the unconscious actors [14]. Often it is seen that the service providers don't take the responsibility of such acts. There is no common consensus between nations regarding cybercrime and every nation puts forth its own interest when such issue arises. No assistance is provided to the investigators. It is so astonishing that even the National Crime Records Bureau (NCRB) has failed to maintain separate record of cybercrimes and it is so unbelievable that in some of the states, not a single case has been recorded. Actual depiction of the number of cases is not there. Due to anonymity and pseudonymous IDs it is very easy to hide identity while performing criminal activities. It becomes really difficult to catch such offenders. There are not enough number of cyber cells across the country. There is a lack of female judge as well to deal with such cases. Till now police are also not well equipped with the technology to catch the offenders and they still lag behind in the digital advancement.

Suggestive Methods to Deal with the Cyber Crimes

i. A wider and a uniform jurisdiction is needed which is called as cyberspace and localization of laws should take place.
ii. Although not everyone misuses the anonymous ID but license should be authorized after thorough examination of the individuals so that pseudonymous IDs could be identified and could be checked.
iii. The terms like 'obscenity' should have universal identification and the term should be defined clearly in order to identify which acts and material are obscene. As there is no punishment for possession and browsing of such materials, now there is a need to keep a check on the knowledge and possession of such contents.
iv. Often the intermediaries remain unidentified. These intermediaries copy and transmit obscene materials from the host. Even if the host is grasped these intermediaries are not traced. An effective system should be developed for tracing and targeting these intermediaries so that the material doesn't get transmitted on a large scale and a major damage could be prevented. The effect of the criminalization of such offence should such that it provides sanctions against intermediaries who knowingly hosts or caches obscene material and those who act as transmitters.
v. The service providers should also be made answerable for their sloppy management and failure for not combating such transmission from their servers. The operators should vicariously be held liable for such activities. Not only the IT cells but the directors are also responsible for the cyber security. Every possible thing should be done to trace the source of the information. The service provider may be held responsible by compelling him to

reveal the identity of the owner of anonymous home page during investigation.

vi. There is a need create an awareness among the international community that a hacker should not be allowed to get away only because of legal inadequacies. An International co-operation in fighting the threat of cybercrime is the need of the hour nowadays, as the cybercrime knows no boundaries and is extensive to the whole world.

vii. The process of reporting the cases should be simplified for the women so that not a single case goes unreported. The investigation process should also be strengthened.

viii. There should be separate records maintained for cybercrimes. Special judges should also be appointed for proper hearing and fast track decisions on such cases.

ix. Special teams should be made by the central government to check the state records and inspection of the functions by officials. It must be inspected that the laws are implemented in the ground level.

x. Digital Police Portal should also be opened for faster action.

xi. It is needed to collaborate both police force and cyber forensic laboratories together for better investigation.

xii. Using ICTs for prevention because of its remarkable features such as ability to take action from distance, ease of propagation and automation.

The organizations can prevent cyber Crimes in the following way:

In the beginning only there should be proper understanding of the cyber threats. The employees should be subjected to reasonable restriction. It should be the policy that during the work there would be control on the activities of the employees. There is a need to make Acts like Data Protection Act (DPA), HIPPA, etc., mandatory for Indian companies. Adequate training must be provided to the employees in cope up with cybercrime threats and to report immediately. There must be update of security policies of the organization on the regular basis. Women in the organization should be given special emphasis regarding security. Special sessions should be organized for them regarding online safety and their systems should be more secured. The Companies must register themselves with the CERT [15] to stay updated with latest vulnerability and threats. They should perform security audit and implement suitable recommendations. Companies should adopt global security practices.

CONCLUSION

As per the threat of cybercrimes, and for a secure cyber ecosystem, there should be a proper registration of a cyber world participant and there is a strong need of the establishment of a proper regulatory body to monitor such cyber threat. Although the government has taken certain measures with regard to cyber security, but the situation demands more expansive and aggressive measures to meet the rising challenges. Cyberspace is a free flowing, borderless and a global medium for facilitating online connections and communications. Different bilateral agreements signed have only limited scope and are inadequate to deal with cyber security. India needs a multilateral treaty which will harmonize its laws by a common criminal policy and deal with international cooperation for combating cybercrimes at global level. There should be strong investigation techniques which can foster international cooperation for combating cybercrimes at global level. National level agencies can develop security guidelines and policy to prevent the users from cybercrime. To help them escape the darker side of this virtual life the legislators need to provide for establishing separate forums for such issues and also get special officers appointed for the purpose. Violation of privacy and nasty intention to harass women through cyber means, cyber stalking and any other form of cybercrimes erodes the possible capacity of Internet in striking a proportionate balance. Digital world offers a variety of opportunities for equal female participation in different fields and facilitate them to work flexibly and distantly thereby improving their financial autonomy. Violence against women is a very serious

nationwide problem which extends to the digital world as well.

REFERENCES

1. Women in the Digital Age, Final Report of European Commission, (http://www.media 2000.it/wp content/uploads/2018/03/Wom eninDigitalAgeStudy-FinalReport.pdf)
2. MacGraw D, Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail, 1995 Rutgers Computer and Technology Law Journal 492.
3. David Harvey, Cyberstalking and Internet Harassment: What the Law Can Do, pg.1.
4. Talat Fatima, Cyber Crimes, pg. 84, (2nd ed. 2016).
5. Peter Stephenson, Investigating Computer Related Crime (CRC Press, Washington DC, 2000) 3.
6. Oxford dictionary
7. Anticybersquatting Consumer Protection Act USC 15, 1999.
8. India's Computer Emergency Response Team- India, 2018 https://www.cert-in.org.in/ItNewsArchive.jsp
9. Cybercrimes and challenges ahead- Vivek Duhapade, pg.5 https://www.research gate.net/publication/265166983_Cyber_Cr ime_and_Challenges_Ahead.
10. Kochhar and Co., Data Security and Cyber Crime in India (Oct 29, 2018), https:// www.lexology.com/library/detail.asp
11. The Information Technology (Amendment) Act, 2008, Section 75.
12. Sharma, S.K. (2013). Tumhari Sakhi. New Delhi: Bukaholic Publications.
13. Information technology Law and Practice, Vakul Sharma 3rd edition, Universal Law Publishing Co.
14. Internet Law Text and Materials, Chris Reed, Second edition, Cambridge University Press.
15. The Computer Emergency Response Teams (CERTs) which has been created in order to coordinate and respond during major security incidents/events. These organisations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stake holders to address these threats.

Cite this Article
Shreya Kaylani, Shambhavi. Women Safety in Digital World. *National Journal of Cyber Security Law*. 2020; 3(1): 47–54p.

