A STUDY ON THE CYBER-CRIME OFFENCES AGAINST WOMEN

Sri Rakshaa. B & Carol James, Christ Deemed to be University, Bangalore

ABSTRACT

"Cyber Crime is the way to jail, cyber security is the way to avail". The authors through this quote in this research paper is primarily focusing on the issues and concerns of Cyber Crime faced by the women in a globalised level. The paper also focuses on few of the 17 Sustainable Development goals with relevance to Cyber Crime which was passed by the UNGA Resolution 70/1 in the year 2015 which is also called as the 2030 agenda. The major goal that has been focused in this paper is Goal no.4 which emphasises on quality education by providing self and societal awareness which in turn results in empowerment of women. The research paper further focuses on the Cyber security laws in India such as the Information Technology Act, 2000. It has also been observed that due to the lack of awareness in women, the female gender has faced suppression and consequently this has also resulted in the increase of crime rate. This Cyber Crime which has recently originated due to the growth of technology, attacks the users by way of hate speech, porn revenge, email spoofing, stalking and Identity theft. It has also been observed in the research paper that Goal no.16 which ensures Peace, Justice and Strong Institutions focuses on evolving women from their submissive stage to the empowered stage. The authors have also critically analysed the loopholes in the existing cyber security laws and have also provided adequate recommendations in order to combat the security issues faced by women.

Keywords: Sustainable development goals, united nations, empowerment, cyber crime, cyber security, Information technology act, 2000

INTRODUCTION

Cyberspace is a complete virtual space which uses machines for receiving, storing and sending information. Such information can be manipulated, published by using computer or network as a source, tool or target to commit atrocities against women in cyberspace. These atrocities are largely referred to as cybercrimes. Cyber crimes are crimes committed with the use of computers or relating to computer, especially through Internet.[1] The various forms of cyber space violations portray various forms of indecent representation of women which are circulated in the cyber world. The Indecent representation is the *depiction in any manner of the figure of a woman, her form or body or any part thereof in such a way as to have the effect of being indecent, or derogatory to, denigrating, women, or is likely to deprave, corrupt or injure the public morality or morals."*[2] Considering the factors that are mentioned, the authors are majorly focusing on quality education as a tool to curb cyber space violations.

Cyber crime- A hindrance for the nation:

Cyber Crime not only affects women but it is also a threat for the entire nation. Cyber attacks may either be malware or denial of service attacks. Malware is a code designed generally to cause harm on data, hosts and networks. This is done whenever a user accesses a corrupt website or downloads an email attachment. The two popular forms of malware such as virus and worms easily spread in a computer and can attack the data. In a denial of service attack the perpetrator launches lump sum fake requests from a single source which in turn temporarily blocks access to the target system. Under both these methods, the perpetrator inflicts harm to the target system thereby causing harm to the data.

Impersonation and Cyber Crime:

In the current digital world, digital identity theft also known as digital impersonation has become a growing concern. Most of the perpetrators use phishing as a vehicle to obtain personal information through fraudulently sending emails purporting to be from reputable companies. The users assuming the same from reputable companies provide access to their personal information and the perpetrators gain such information through fraudulent misrepresentation. Even though most of the identity theft scenarios aim at making money, money does not become the sole aim in these cases. Harming, harassing or bullying someone anonymously is few other

[1] The Cambridge English Dictionary
[2] Section 2(c) of the Indecent Representation women (Prohibition) act,1986

motives of this crime. All of such cybercrimes not only hinder the development of a nation, but also cause threat to individuals. Both men and women are hugely affected due to cyberspace violations. However, this article will specifically deal with respect cybercrime violations against women.

Objectifying women:

Objectification is treating a person, usually a woman, as an object. Sexual objectification plays a vital role in gender inequality. Identifying a woman through her physical characteristics not only affects her in losing individuality, but also leads to psychological ailments. Many of these directly connect to sexual victimization. This in turn leads to passing sexual jokes or comments over the internet, slut shaming or body-shaming, porn-revenge, morphing, threatening, torture, cyber-defamation and other harassments against women in the cyberspace. These harassments tend to outrage the modesty or dignity of a woman and therefore constitute a violation of their human rights and fundamental freedoms. Also, women need not be an internet user in order to encounter the violence of cyber crime. They can be objectified and published through depiction of rape videos and by circulating the same over the internet. They may also become the products sold through online websites which encourage human trafficking and sexual slavery.

Cyber Space violations :

i. **Pornography:**

Pornography means showing sexual acts through obscene websites or obscene materials produced by using computers and also includes downloading or transmitting pornographic videos, pictures and writings. The context of obscenity as an offence has been mentioned in Section 292 of the Indian Penal Code and Child pornography as an offence is provided in Section 67B of the Information technology Act, 2000.

ii. **Doxxing:**

Doxxing is the publishing of private or identified information about a particular person with a malicious intent. Under the Indian legal system, the laws to combat doxxing is covered under the ambit of (i) The Information Technology Act, 2000 Sections 66 A – 66E and 67, (ii) The Indian Penal Code – Section 354C, 354D and 500.

iii. Cyber defamation:

Cyber defamation takes place with the help of the computers or the internet, whenever a perpetrator publishes a defamatory matter or sends it via e-mail to their friends. The so called information is published through the internet thereby tampering the image of a person and thereby causing harm to their reputation. This is provided under Section 509 of the Indian Penal Code which provides uttering any word or gesture intending to outrage the modesty of a woman.

State of Tamil Nadu v. Suhas Kutti [3] is a first case of conviction under section 67 of IT Act, 2000 in India. In this case, some defamatory, obscene and annoying messages were posted about the victim on a yahoo messaging group due to which the victim started receiving annoying calls. She filed a FIR and accused was found guilty under sections 469, 509 of the Indian Penal Code 1860 and section 67 of Information Technology Act.

iv. Morphing:

Under morphing, the perpetrator downloaded from websites by fake users and are edited and modified in order to publish fake images over the internet. This amounts to violation of I.T. Act, 2000. The violator can also be booked under IPC also for criminal trespass under Section 441, Section 290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation Criminal law amendment bill, 2013

The Criminal law amendment bill, 2013 was introduced pursuant to the brutal gang rape case called Nirbhaya rape case. This bill introduced brought in certain new category of offences into the Indian penal code and made sexual voyeurism and stalking as an offence. It has been one of the most concrete steps taken by the Indian government to curb violence against women.

v. Sexual harassment- Section 354A :

The Indian case of *Vishaka v. State of Rajasthan*[4] highlighted a major aspect concerning sexual harassment. It stated that a demand or request for sexual favours certainly amounts to sexual

[3] State of Tamil Nadu v. Suhas Kutti
[4] Vishaka v. State of Rajasthan

harassment. Through this case it can be inferred that if the demand for sexual favours is made through the usage of online portals, the same will amount to a Cyber Crime.

vi. Voyeurism:

Any man who watches or captures image of a woman engaging in a private act which she would not have expected may amount to voyeurism as specified under Section 354-B of the Indian penal code. If such image is being circulated over the internet, the same would amount to Cyber Crime.

***vii.* Stalking – Section 354D:**

It means following a person and making or attempting to make contact despite a clear disinterest being displayed by the other person. Stalking may be committed both physically and through electronic media against women.

United Nations opinion on the cyber violence against women and girls:

1. A major societal and economical issue to be addressed at the global level is cyber violence against women and girls. On analysis, it has been observed by the United nations that the statistics collected reflects a threat on the peace and security of nations which is the core ideology of the charter of United Nations. Apart from this, it is also violating the goal of Gender equality and empowerment of women which is enshrined as one of the 17 Sustainable Development goals by the United Nations.

2. The United Nations system had taken a joint effort in the 21st century to establish a sustainable development paradigm with the core principles of gender equality which ensures Peace, Justice and Strong Institutions, adequate literacy on the access of technology. In order to eradicate the endemic violence against women and girls, all interest holders are firmly obligated to take accelerated actions to ensure a safe and secure access to the medium of internet for the present and future generations.

   Outrages upon personal dignity under International law:

3. In Aleksoviski, the Trial Chamber quoted that "Outrages upon personal dignity refer to those acts which do not directly cause harm to the physical or mental well being of a person. But the said outrage in turn humiliates and ridicules the individual. It has thus

considered these factors as a key for establishing the elements of this offence.[5] The principle of respect for human dignity is intended to shield human beings from outrages upon their personal dignity, whether such outrages are carried out by unlawfully attacking the body or by humiliating and debasing the honour, the self-respect or the mental well-being of a person.[6]

Elements for outrages upon personal dignity:

(i)That the accused intentionally participated in an act even after knowing that the act would cause serious humiliation, degradation or otherwise be an attack on human dignity. (ii) The perpetrator or the accused also knew the consequences of the said crime indulged.[7]

If the perpetrator intentionally body shames or slut shames a woman by passing derogatory remarks against her character with a clear knowledge of his act and the consequences of the same, he is said to have outraged the modesty of a woman.

Cyber Crime issues at Individual Nation level:

Every nation has introduced certain measure in order to curb Cyber Crime violence against women. The remedies to curb Cyber Crime fall into three broad categories: 1) Providing assistance to the victims of Cyber Crime through various schemes. 2) Analyzing the exiting substantive and procedural law and amending the same in order to suit the needs of the society, 3. Providing awareness and training through education.

INDIA

The Indian Government has established cyber cells and cyber police stations in order to investigate these crimes. The Government has circulated computer security policy to all ministries/departments in order to prevent, detect, mitigate and reduce Cyber attacks. Further, the Indian government has also enacted The National Cyber Security Policy, 2013 in order to build a secure and resilient cyberspace.

U.S.A

[5] Aleksovski trial judgement para 55
[6]Furundzija Para 181
[7] Kunarac et al. Para 514

In 2008, Congress passed a law requiring sex offenders to provide information about their online identities to State sex offender registries. This information will be provided to the Attorney general who will in turn maintain a secure system through which social networking sites can compare the information contained in the National sex Offender registry.

UK

UK attempts to raise public confidence and awareness. It also aims at working internationally to tackle Cyber Crime with successful liason between all groups working to protect the public. It also tries to review all the existing legislation in order to ascertain whether that particular legislation can address the relevant need.[8]

Recommendations by the Special Rapporteur at the UN level:

a. States should modernize and amend existing legislation according to the need of the society.

b. Intermediaries engaged in the moderation of online conduct should ensure clear and comprehensive content moderation policies

Media's role in circulation of Hate speech:

1. Media is both a boon and a bane. The greater the platform it provides for expressing an individual's opinion, the more it initiates tensions in the society. These tensions may arise due to misinformation, false propaganda, passing derogatory comments over the internet and instigating hate speech.

2. In the case of Prosecutor v Jean Paul Akayesu,[9] The RTLM media has instigated hate speech against the Tutsi group which were the minorities in Rwanda. This incited genocide and the commission of various other acts such as rape, sexual harassment and outraging the modesty of women etc., in order to destroy the tutsi group as such. [10] One recent issue is the Rohingya issue wherein the social media had exaggerated the problem. The hate speech in that case, was targeted mainly towards ethnic communities which were in turn propagated through social media outlets. The content

[8] (https://assets.publishing.service.gov.uk/government/uploads/system/upload)
[9] ICTR-96-4-T
[10] Prosecutor vs. Jean Paul Akayesu , ICTR

was circulated on facebook and it did not have enough local moderators in Myanmar to tackle the issue, the accounts and posts more effectively. This issue highlights the role of the media in influencing the society. When major media outlets don't take enough measures to verify the source of their information, the issue of accountability cannot be taken into consideration.

3. Right to expression has grown so much that all other rights are getting affected in order to uphold that particular right. The freedom of expression over the internet is available to every individual. But any opinion expressed due to a right conferred on one sect on the society should not harm or psychologically affect another sect of the society. Any form of portrayal of a woman in an inappropriate manner affects her individual dignity. A media influences the society as such. In accordance with such influence, it plays a decisive role in the society. This decisive role should be used in portraying women in roles that are positive rather than tampering their image.

RECOMMENDATIONS:

Media's role in content moderation:

Media necessarily plays an active role in content moderation. The individuals especially women are expected to communicate whenever there is a threat to them via social media and to take measures in order to protect themselves by disclosing their personal information only to the people they know. Even though this step can be taken by women, it is also on the part of the media to ensure that their users are not under threat whenever they use the social media. For this purpose, the social media should regulate and moderate the content received by them.

The initiative can be taken by pre-moderation wherein social media checks the reviews or photos whatever received and don't disclose offensive contents or blocks such content. Another appropriate method is the post moderation wherein which the moderator gets the right to add or remove the content. Post moderation is usually considered as a better alternative compared to pre-moderation since the moderator can immediately reject or accept a particular content after it gets posted on the internet. Yet another type of moderation is the reactive moderation wherein the members themselves become responsible whenever they feel that a particular content is inappropriate. Many of the recent apps have enabled new features such as reporting a particular fake account, enabling the feature of encryption and also by blocking offensive content over the internet.

Finally another alternate strategy recommended for adoption by the social media is the use of automated moderation. In the case of automated moderation, there are lists of banned words which are entered, and whenever a message is being typed the tool either replaces it with some other alternative or either rejects it or blocks that message altogether.

CONCLUSION

"Educate, empower and enlighten women in order to eradicate crimes against them". On observations conducted by the researchers it can be concluded that several initiatives were already taken by various nations to tackle crimes of female foeticide and cyber crime. Yet there are some lacunas and the researchers have put in their maximum effort to provide further recommendations to resolve the crime of female foeticide, infanticide and cyber crime by quality education as an instrument. Finally, the authors concludes the research on resolving female foeticide and infanticide, cyber crime by emphasising on the quote " Don't wait for a global change, rather initiate a change towards the globe"

REFERENCES

i. ARTICLES:

Indecent Representation women (Prohibition) act,1986

ii. CHARTERS AND STATUTES:

1. Universal Declaration of Human rights, 1948
2. International Convention on Civil and political rights, 1966
3. Charter of United Nations, 1945
4. Rome Statute of the International Criminal Court, 1998
5. Indian Penal Code, 1860
6. Indecent Representation women (Prohibition) act, 1986

iii. CASES:

a. INDIAN CASE LAWS

1. State of Tamil Nadu v. Suhas Kutti
2. Vishaka v. State of Rajasthan

b. INTERNATIONAL JUDGEMENTS

1. Prosecutor v. Aleksovski
2. Prosecutor v. Furundzija
3. Prosecutor v. Kunarac et al.
4. Ntagerura, Bagambiki, and Imanishimwe
5. Prosecutor v Kordic and Cerkez, (Appeals Chamber), December 17, 2004
6. Prosecutor vs. Jean Paul Akayesu

iv. RESOLUTIONS:

1. UN General Assembly Resolution 51/76

2. UN General Assembly Resolution 70/1