VOL.3 ISSUE 2
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

VICTIMIZATION OF WOMEN IN CYBERSPACE: A CRITICAL STUDY OF THE GAPS EXISTING IN THE LAWS IN INDIA

-Ms. Shipra Chauhan [1]

ABSTRACT

Information dissemination has become easier with the advent of technology. But usage of computer, internet and mobile services has been not without its ramifications. Cyber enabled crimes have grown and unfortunate number of women are becoming victims of cyber violence. There is a constant challenge to a women's dignity and privacy in this era of social media. Cyber violence against women through instances of stalking, blackmailing, cyber harassment, abuse, voyeurism, body shaming is very much prevalent and the harsh reality is that the much of such cases even go unreported. Cybercrimes relating to women gravely violate body privacy which have severe long term effects. To keep pace with the changing dynamics in the digital domain India enacted its IT Act, 2000 which also made significant amendments to IPC. Most of the cybercrimes against women are registered under the IT Act but still there exist a lot of impediments in the form of lack of awareness and infrastructure, inadequate criminal justice response and gaps in the legal framework. Effective policy interventions are required. The paper will discuss traditional forms of cybercrimes and the adaptive forms of cybercrimes against women. The paper will also focus on the need for developing protective strategies for people realising the fact the victims of such crimes are largely women. It has been a decade since the IT Act, 2000 was amended and the Act seems to lag behind in providing adequate protection to women who become the victims of cyber crime. The paper will further suggest a need for necessary changes in the Act to be in accordance with the rapidly advancing technology and to effectively deal with the creative ways of committing crime using such technology.

Key Words: *cyber violence, cyber harassments, legal inability, IT Act, 2000*

[1] Assistant Professor(Law), SYMBIOSIS LAW SCHOOL, HYDERABAD

Introduction

Computers and internet are considered to be one of the greatest gifts of technology to mankind. In this information and communication technology age, internet has become a boon for the society. Internet has provided alternate forum for banking services, health care, transportation, financial planning and at the same time has made communications easy by establishing a virtual space. The level of communication has gone higher through computer as now you can be connected with friends and family around the world. In today's scenario many business transactions and proposals are executed with the help of computers. In simpler terms internet and computers has made our life easy where we can order food online, shop online, pay bills online while enjoying the comforts of our home. Computers have also influenced Print media, Television and Radio communication in a vast manner. Social networking sites like, Twitter, WatsApp, Youtube and Facebook have opened yet another platform for viral communication overcoming the difficulties in the form of distance and time. But all these pros do come with the cons. We need to remember that it is not the computers or the internet that commit crimes, instead internet creates opportunities for criminal masterminds to misuse the technology. Internet acts as a haven for such criminals.

The increasing use of technology and the Internet in all aspects of daily life puts everyday citizens at risk of becoming targets of cybercriminals. Cybercrime has become a real threat. The threats posed through internet as a medium come in a variety of forms and the users and also other technological devices. Cyber enabled crimes pose a much serious risk and threat to children and women which are the more vulnerable in such a scenario. The contents and wide diffusion of social media have not only reinforced existing forms of violence against women, they have also created new tools to threaten women and inflict harm, both offline and online.[2] Women's human rights have evolved greatly in the past two decades, both globally and in India. However, gender inequality is still pervasive in every dimension of society. This reverberates in the online world. Cyber violence against women and girls is emerging as a global problem with serious implications for societies and economies around the world. Research studies conducted and the statistics so collected clearly depict that cyber violence targeted towards women risk the peace and prosperity for all enshrined in the Charter of the

[2] UN Broadband Commission for Digital Development (2015), "Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call", available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

United Nations, and, in particular, to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement.[3] The situation regarding cyber violence against women and girls becomes more grim when perpetrators of such crime are rarely held accountable in part due to the relatively low capacity to prosecute offenders.

The paper in the first part will discuss various kinds of cybercrimes against women and their changing trends. Although online violence can take on various shapes, e.g. sexual harassment, image based sexual abuse or sexist hate speech, experts are now recognising these forms of cyber violence and hate speech online against women as part and parcel of a continuum of violence, often starting offline and reverberating online and vice versa, pushing back women from public spaces to the private sphere. The paper will also focus on the impacts of such crimes on women and girls and the remedies existing in laws in India. The last part will shed light on crime violence situations around the world and the author will propose certain recommendations and suggestions.

Defining cybercrime and its variations.

During the initial period of the occurrence, the term "Cyber Crime" was never defined by any legal provisions, Bills, draft laws or conventions. Many of the academicians and computer specialists involved lot of efforts to analyze and define the term "cyber crime". In simpler and basic terms, it was understood as (i) attack on the "machine" and (ii) computer assisted crimes. The trend of defining cybercrime saw a metamorphosis in the new millennium. Prior to 2001, most definitions explained cyber as a medium of attack on commercial ventures and security breaching techniques like hacking and cracking. The Convention on Cyber Crime (2001), broadened the term by including crimes against children done through the internet and also slightly touched on attacks on human emotions, banning usage of "improper words" in the cyber space.[4] Hence, there was a transformation in understanding cybercrime from the perspective of the victim, an approach which was absent in earlier definitions.

Cyber crime or Cyber violence is a form of Gender-Based Violence (GBV). Cyber violence can be understood as offences that are committed against individuals with a criminal motive or intention to denigrate the reputation of the victim or cause physical or psychological harm

[3] *Supra* 1
[4] Halder, D. and Jaishankar K., Cyber Crime and the victimization of women: Laws, rights and regulations, Information Science Reference, 2012.

to the victim directly or indirectly. Such violence can be perpetrated by using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).[5] The term "cyber violence" encompass different types of cyber violence such as cyber harassment, cyber stalking, non-consensual image-abuse, and also the specific term "sexist hate speech". There is however no commonly accepted terminology for these relatively new forms of violence against women. The recent report from the Special Rapporteur on Violence against women presented to the Human Rights Council in June 2018[6], recalls that "terminology is still developing and not univocal". The Special Rapporteur uses the definition "ICT-facilitated violence against women" but also employs the terms "online violence against women", "cyber violence" and "technology-facilitated violence". Online violence against women is defined in the report as "gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.[7]

Online platforms where these various forms of violence and abuse occur include social media (e.g. Facebook, Twitter, Instagram), websites and other discussion sites, search engines (e.g. Google), messaging services (e.g. Whatsapp, Facebook Messenger, Snapchat or Skype), blogs and dating websites, comment sections of media and newspapers, gaming forums. Often, existing definitions of gender based violence and cybercrime are extended in order to grasp the phenomenon of cyber violence and hate speech against women and the different types as cited above.[8] Some of the newer forms of cyber violence against women can be placed in distinct categories as sexual crimes, non-sexual crimes.

[5] Halder, D. and Jaishankar K., Cyber Crime and the victimization of women: Laws, rights and regulations, Information Science Reference, 2012.
[6] Human Rights Council (2018), thirty-eighth session, 18 June–6 July 2018, "Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective", available at https://www.ohchr.org/EN/HRBodies/HRC/.../Session38/.../A_HRC_38_47_EN.docx
[7] *Ibid*
[8] European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, 'Cyber violence and Hate speech online against women', available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

1. Cyberbullying

It can be defined as the "*repeated verbal or psychological harassment carried out by an individual or group against others*".[9] Both men and women can be perpetrator while bullying women. Perpetrator may target the victim with obscene/vulgar remarks. Bullying may further involve comments regarding her personal life. Bullying may lead to online defamation and infringement of privacy as the bully may play lead role in leaking the personal information of the victim in the web. Much conduct that has been described as cyber-harassment involves mobbing behaviour aimed at silencing women and racial minorities, which seems cross the line between bullying and harassment.[10] According to various studies, cyberbullying differs from face-to-face bullying in various aspects such as the internet provides anonymity, lack of any sense of hesitation or responsibility on part of the perpetrator, the capacity to reach a wider audience, and the reluctance of victims to report incidents of cyberbullying. It can in certain scenarios also include gender based hate speech targeting the individual victim.

2. Cyber stalking

It can be defined as "involves repeated incidents, which may or may not individually be innocuous acts, but combined they undermine the victim's sense of safety and cause distress, fear or alarm. It can include sending emails, text messages (SMS) or instant messages that are offensive or threatening; posting offensive comments about the victim on the internet; and sharing intimate photos or videos of the respondent, on the internet or by mobile phone".[11] Most researchers believe that cyber stalking is cyber harassment which includes continued unwanted contacts. Cyber stalking can take place through email communications, social networking sites, chat room communications. Such kind of cyber violence can go on for a long period and can lead to the victim developing psychological problems.

3. Malicious Distribution:

The use of technology to manipulate and distribute defamatory and illegal materials related to the victim and/or VAWG organizations; e.g., threatening to or leaking intimate photos/video;

[9] European Parliament (2016), Study for the Libe committee, "Cyberbullying among young people", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf
[10] Jacqueline D. Lipton, Combating Cyber Victimization, Berkeley Technology Law Journal, Vol. 26, No. 2 (Spring 2011).
[11] EIGE, Gender equality glossary and thesaurus, available at http://eige.europa.eu/rdc/thesaurus

using technology as a propaganda tool to promote violence against women.[12] Malicious distribution can also include 'revenge porn' consists of an individual posting either intimate photographs or intimate videos of another individual online with the aim of publicly shaming and humiliating that person[13], and even inflicting real damage on the target's 'real-world' life like the victim getting humiliated in front of co-workers.

4. Cyber Impersonation

The use of technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents; e.g., sending offensive emails from victim's email account; calling victim from unknown number to avoid call being blocked. In certain scenarios, perpetrators also impersonate the victim, largely women through media and subsequently contact the victims' friends and family with a fabricated story that the victim is in danger and in dire need of money.[14]

Law on cybercrimes against women

In India, cybercrime against women is relatively a new concept. When India enacted its very first law in the field of information technology, the immediate need that was felt was to protect the e-transactions and electronic commerce related communications. The drafters could not for see the fact that internet and cyberspace can act as tools to violate privacy of victims especially women and to perpetrate cyber violence against women. The drafters of the Indian Information Technology Act, 2000, created it on the influence of the Model Law on Electronic Commerce, which was adopted by the resolution of the General Assembly of the United Nations in 1997. While commercial crimes and economic crimes were moderately managed by this Act, it miserably failed to prevent the growth of cybercrime against women.[15] The term 'cybercrime against women' in India is mostly used to cover sexual

[12] UN Broadband Commission for Digital Development (2015), "Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call", available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

[13] UN Broadband Commission for Digital Development (2015), "Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call", available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

[14] Lipton. Jacqueline D., Combating Cyber Victimization, Berkeley Technology Law Journal, Vol. 26, No. 2 (Spring 2011).

[15] Halder, D., & Jaishankar, K. (2008, June). Cyber crimes against women in India: Problems, perspectives

crimes and sexual abuses in the internet, such as morphing the picture and using it for purposes of pornography, harassing women with sexually blackmailing / harassing mails or messages etc, or cyber stalking.[16]

The situation related to the prevention of cybercrimes against women and their protection changed during the period of 2006-2008. With the introduction of necessary amendments in Information Technology Act in 2008, India witnessed installation of cybercrime police cells in various States of India. This created a lot of awareness and also encouraged the victims to approach the cybercrime cells through online form-fill up facilities. Still, the concept of cyber victimization remained to be used mainly for covering financial data theft and cyber sexual offences including stalking. In these situations, cybercrime related laws were hardly used due to lack of suitable provisions in the IT Act. The Act earlier had only two sections i.e, s. 67 on obscenity and s. 72 on breach of privacy that dealt with cyber violence but still did not distinctly referred to women as victims in such cases. With regard to the legal protection afforded to cyber victims, the 2008 amendment made in the IT Act has recognised certain offences on the lines of cyber harassment and cyber bullying. Using slangs, name calling, slut shaming and body shaming for women are also widespread in Indian social networking sites, chatting sites etc.

S. 502 IPC may serve purposes for preventing adult bullying, hate propaganda or offensive mails[17], but harassment of women are not mentioned here. Cyber harassment can be punishable under s. 509 IPC, which prohibits uttering any word or making any gesture intended to insult the modesty of a woman.

Apart from this one has to remember that all cases of cyber harassment, cyber bullying and cyber impersonation clearly violate right to privacy which has been lately recognised as a fundamental right u/A 21 of the Constitution by the *Puttaswamy judgment*[18]. These offences also impact and violate right to life u/A 21 of the Constitution.[19] The concept is equally

---

and solutions. TMC Academy Journal, 3(1), 48–62.

[16] Balakrishnan, K. G. (2009). Speech at seminar on cyber crimes against women - Public awareness meeting, Maharaja College, Ernakulam, August 1, 2009. Retrieved on 6th July, 2010,

[17] Section 502 (b) prohibits sale of printed or engraved substance containing defamatory matter knowing it to contain such matter in any other case and terms it as a non-cognizable offence with simple imprisonment for 2 years or with fine or with both.

[18] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors, (2017) 10 SCC 1

[19] Right to life was first interpreted to cover life with dignity in the case *of Maneka Gandhi vs. Union of India*, AIR 1981, SC 746. In this case, the court held that: "right to live is not merely confined to physical existence, but it includes within its ambit the right to live with human dignity".

applicable in cyberspace. Various sorts of cyber offences of the nature of invading privacy, such as stalking, floating private information in the web without consent, unauthorized accessing and modifying digital contents and misusing them, may crop up only when these two basic rights are hampered.[20] Section 65 further prohibits tampering or modification of such data that were accessed unauthorized. Further, section 66 C can also be applicable in case where victim's account is 'taken over' and misused. Though the section is meant to control bank frauds, credit card frauds and email account hackings but it can be broadly interpreted to cover cyber offences in the nature of hacking and impersonation of female victims.

Regarding cyber stalking, t is curious to note that S. 354D[21] of IPC which was added by Criminal Amendment Act 2013 post *Delhi gang-rape case* takes into account both, the physical stalking and cyberstalking. The provision clearly mentions that if anyone tries to monitor the activities of a woman on internet, it will amount to stalking. The perpetrator shall be guilty of the offence under Section 354D, IPC. Further, Section 67A of IT Act, 2000 relates indirectly to cyberstalking. Added after the 2008 amendment, the section states that if stalker attempts to publish any "sexually explicit" material in electronic form i.e., through emails, messages or on social media then he shall be guilty of an offence under Section 67A of IT Act and shall be punished accordingly.

Section 67B of IT Act, 2000 focuses on when stalker targets children below the age of 18 years and publishes material in which children are engaged in sexual activities in order to terrorize the children. Section 66E[22] of IT Act, 2000 and Section 354C[23] of IPC deals with "voyeurism."

Recommendations and suggestions

[20] Halder, D. and Jaishankar K., Cyber Crime and the victimization of women: Laws, rights and regulations, Information Science Reference, 2012.

[21] S. 354 D (1) - Any man who—

1. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
2. monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking;…….

[22] S. 66 E- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished.

[23] S. 354 C- Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished….

There seem to be several lacunae and loopholes in the law on cyber violence against women. The provisions of the IT Act, which is the key act dealing with the cyber issues and offences in India does not have any women specific provision. Cyber victimization of women has become so much rampant that there arises an absolute necessity to certain offence under the IT Act as gender specific. Though the amended version of the I.T. Act differentiates child pornography from adult obscenity and pornography but there is no mention of any provision in this Act to protect women distinctly. There is also a requirement to establish a gender centric victim assistance cell. Necessary changes should be made in the IT Act for establishment of such cells as women and girls facing any kind of cyber violence fear the social stigma and rarely report their cases. Moreover, sensitization of the masses should be done to achieve positive public consciousness to ensure that cyber violence against women is neither ignored nor trivialized. In particular, there is a strong need to focus on violence prevention and community mobilization for zero tolerance for violence against women in cyberspace. Also, after the analysis of the IT Act and the relevant sections of IPC, it is crucial to note that, the punishments under the IT Act are much stronger compared to those in IPC. Further, in order to restrict the harassing behaviour of the stalker, few steps should be taken by Internet Service Provider. Few ISPs provide the opportunity to report abuses for example, Facebook has its privacy policy in place and also some safety features that protect the personal information from being downloaded. However, there should be necessary amendment through which responsibility of such ISPs needs be categorically mentioned in the IT Act. Privacy norms should be made stringent and its high time that India should adopt a privacy protection legislation that also discusses and prohibits misuse of information of a person, women categorically that can lead to any kind of cyber violence or cyber victimization. Lastly, substantial training should be provided to all law enforcement personnel regarding protection of victims who have faced some or the other forms of cyber violence. Certain workshops should be conducted for sensitizing police, lawyers and judges such that they are able to rapidly respond to complaints of the women facing cyber violence and also prosecute the perpetrators.

Conclusion

The challenge of keeping up with the technological pace of change will require a parallel pace of change in the social behaviours and norms of netizens, which should also be reflected in the laws. India still needs to recognize that cyber violence against women does not only

signify sexual crimes but it can be of various non-sexual types as well. It can be noted that India manages most gender harassment cases in the cyber space with the help of century old laws, which were created during the British colonization period. India needs more specific laws to cover cybercrimes including stalking, adult grooming, emotional cheating and subsequent harassments etc. Cyber victimization is a worldwide phenomenon and necessary steps in the form of amendment in laws, creating awareness in the minds of people and also the victims, sensitizing the police personnel is required.