National Commission for Women
New Delhi

Cyber Security of Women- A Concept Note

Introduction

Cyber Crime against women is a term used for any illegal activity that uses computer and similar electronic devices e.g. phones, e-mail, internet, social media platform etc. as its pressing tool for offences against of women. It is in a way gender based violence against Women by use of computer and information and communication technologies. It has been significantly increasing over the years, with rising number of internet users in the country. The estimated number of e-literates in the country are around 60 crores now and their number has increased exponentially, as it was estimated to be only 40 crores in 2019. Accordingly to the crime data released by National Crime Record Bureau (NCRB) during 2017, out of 21,796 Cyber Crimes registered in the country, 4242 were committed against women. Moreover, increase in the cases registered during the year 2016 shows an increase of around 77% from the previous year.

2. The nature of Cyber Crimes ranges from petty online frauds to big financial scams and sexual harassment. Since the technology associated with internet and available smart devices are new and are not commonly understood, people are becoming easy prey to the ill designs of cyber-criminals. Women are more prone to such crimes, because of the accessibility with anonymity available in the cyber space. Since one can hide and fake his identity in the internet, the facility is misused by criminally minded persons to commit such crimes.

3. The five most vulnerable States in the Country having highest number of cases of Cyber Crimes registered as per NCRB Reports are Uttar Pradesh, Karnataka, Maharashtra, Assam and Andhra Pradesh, while in case of Cyber Crime against Women, Karnataka and Maharashtra are the State having highest number of registered cases. States also shows a phenomenal increase in number of Cyber cases registered during successive year. In UP, which has the highest number of cases registered during the years 2016, 2017 and 2018 there has been 188% increase in 2017 from 2016 and 126% increase in 2018 from 2017. Similarly, in cases of registered cases of Cyber Crimes against women in UP, the increase in 2018 from the year 2016- 2017 was 128%. The Karnataka, which has the highest number of Cyber Crimes against women, an increase of 173% during 2018 from previous year, has been noted. This is based on the data released by NCRB on registered cyber crimes.

4. It may be noted that the NCRB, data is based on the number of cases registered by Police and is in no way the indicator of actual number of Cyber Crime cases is the society. It is a case of major under-reporting and therefore actual state of affairs in the country in this regard is anybody's guess. Most of the women victims of Cyber Crime do not seek legal recourse for

reason of victim blaming and shamming. NCRB estimated that only 10%, of the Cyber Crime reported, pertain to offences against women.

Social Repercussions of Cyber Crime against Women:

5. Cyber Crimes against Women have detrimental effect on women's wellbeing, their psychological and mental health and their dignity. The constant fear of safety, loss of reputation adversely affects their life. The forms, nature and manner of cyber crimes are constantly evolving, with ever-evolving technology. There are studies to tell that psychological and social consequences of Cyber crimes to victim's life are serious and even potentially incapacitating. Anxiety, sadness, negative feelings, social avoidance and even higher risk of suicidal attempts are reported. Moreover, it has become a question of deprivation of rights of women ever since the UN declaration of right to internet as a human right for women. The psychological trauma to women gets aggravated multifold, when the Cyber Crimes are not committed by strangers but many a times the perpetrator is intimately known to the victim and sometime he is even partner or former partners. As such, the harassments are not limited to online platform but also involve threat of physical harms. The Cyber Crime, therefore, gets mixed up to become both online as well as off line.

6. The Cyber Crimes against women are also being used as a powerful tool of social censorship to a women's voice as her right to speech. The sexist and misogynistic language used by the perpetrator of the crime is also intended to silence women's voice.

Types of Cyber Crimes against Women and available Legal Remedies:

7. Following are some typical forms of cyber crimes against women in the country and the legal remedies that are available to contain the menace:

(i) Cyber Harassment: It is a repetitive online behavior intended to disturb a person and in case of women harassment is often sexual in nature and mainly involves persistent and unwanted sexual advancement through different platforms including e-mails, messaging social-media, chat rooms, gaming etc, where people participate by way of showing the content/views. It involves posting, sending or sharing negative, nasty, false information about someone for causing humiliation and character assassination. It becomes difficult to track down the culprits, as it is often done though fake identities, sometimes even through multiple fake identities. The magnitude of cyber harassment/bullying is quite significant and courts also take such offence seriously, as even compromises arrived with the women and accused and subsequent request for questioning the proceedings was not accepted by Maharashtra High Court (Shreya Singhal Vs UOI). The offence of trolling, bullying and black mailing are dealt with the provision in IPC for criminal intimidation though anonymous communication (Section 503, 504 and 507 of IPC) and Section67 of the IT Act 2008.

(ii) Cyber stalking: Cyber stalking involves persistently following a person's movement for a long time across the internet by various methods for tracking her online behavior e.g. messaging

on the bulletin boards frequented by the victim, constantly sending e-mail to the victim. It usually occurs with women, who are stalked by men and is aimed at tormenting or terrorizing the victim. The motives behind a man for cyber stalking women are usually (i) sexual harassment, (ii) obsession for love, (iii) revenge and hate or (iv) ego and power trips. A stalker usually follows the victim everywhere and threatens her by repeatedly calling her, or sending messages through e-mail, SMS. The stalker usually creates a fake profile on social media to approach the victim. He even uses the profile and photograph of another person to pose and falsely project his profile as a real one. The stalker keeps an eye on the activities of the victims from their check in the social media such as facebook, instagram etc. and gauge the behavioral pattern of their victim, quite accurately. With the victim's address, the stalkers even find the surroundings of the victim by using Google map street view. Some tech–savvy stalker can find it from the photos posted by the victims on the social media through the geo-tag of the photo, if it is digital, as then it contains details of time and location of the pictures, which can be read with the help of special Apps. Even stalkware are available, which is a type of spyware and tracks the location, enables access to text and browsing history, and even makes audio recording, without any knowledge of the victims.

Cyber stalking is blatant intrusion into individual's privacy, most frequent reported. Section 354 D of IPC, which defines and provides for punishment of the offence of stalking man who follows a woman, contacts her or attempts to contact her for personal interaction repeatedly despite a clear disinterest from such woman, monitors the use of internet, email or any other form of electronic communications, after hacking/cracking her personals and theft of her identity.

(iii) Cyber Pornography: Cyber space is used to generate design distribute, display or import obscene material. This action is another big threat to the women netizens, as they do not know what actions of theirs are being recorded and would end up on internet. Moreover, the pornography videos have aggression as the prime content and a definite correlation has been found between pornography used and cases of violence against women. The porn also generate new expectations of sexual behavior from women, which may lead to higher divorce rate, infidelity etc. There are various other social implications of pornography on women. It reflects sexually explicit subordination of women, de-humanizing of women by treating her as a sexual object or commodity.

Cyber pornography has therefore, been covered as a crime under Section 67 of IT Act 2000, although it is also covered and punishable under various sections of IPC e.g. 292, 292A, 193 and even 509 (outraging the modesty of women). Additionally, Section 354 A of IPC inserted in 2013 deals with sexual harassment by way of showing pornographic material to a woman against her will, a provision useful when whatsapp, e-mail or other means are used for the purpose. Section 67A of the IT Act also prohibits publishing and transmitting in electronic form any material which contains sexually explicit act or conduct as a punishable offence.

(iv) Morphing : Editing the original picture of a women and morphing it by use of technology with another picture and then resorting to blackmail with a threat to release the morphed picture

is another common crime against women. Women's picture available on social media is generally used for this purpose. The incidents of morphing are increasing by being used against celebrities, who are easy prey, but even ordinary women are targeted for black mailing, taking revenge and to harass/tarnish the image of a woman in her family/friends/social circle.

Morphing the image of a woman and creating/distributing and sharing it as a non-consensual image even if it is not a pornography also needs to be regarded as crime against women. Though 'morphing' as such is not mentioned in IT Act 2000 or any other law and is not recognized as a crime, but it may be regarded as a tool used for committing crimes against women and the offender may be booked on the intention for which the morphed image is used or threatened to be used.

(v) Email spoofing: Fraudulent e-mail activity in which sender addressed is altered to conceal the actual sender is called e mail spoofing. Fake identities for such mails are generally used to extract personal information and private images, of unsuspecting women, which are ultimately, used to blackmail the women. E-mail spoofing and impersonation attracts provisions under Section 415 and 416 of IPC under the category of cheating and impersonation. It is also covered under Section 66 D of the IT Act.

(vi) Voyeurism: It involves violent invasion of the private space of a women by a man. The act is covered under Section 354C of IPC and its features are capturing and disseminating image of woman engaging in a private act without any expectation of being observed. The act is punishable under Section 66 E of the IT Act.

Gaps in Existing Legal Frame work:

8. It is evident from above discussion that the provisions in IPC and IT Act, both are applied to the cyber crimes cases against Women. In cases of many Cyber offences against women, the provisions of the two Acts are applied by way of interpretation, due to lack of specific provisions for specific cyber crime committed against women. The IT Act contains a chapter on offences and computer related offences, but the provisions mainly deals with economic and financial issues and not cyber crimes against Women.

9. The main sections of IPC provided after Criminal Laws (Amendment) Act 2013, as applicable to Cyber Crimes against women are 354A, 354C and 354D and 509. It is clear that IPC, the general criminal law of the land, defines a large number of offences and prescribes punishment for them. However, the provisions primarily address crimes committed in tangible/physical form. These provisions are also applied to cyber crimes against women by way of judicial interpretations, although specific provision is available to cover sexual harassment including showing pornography against the will of women, voyeurism including watching, capturing & disseminating of private act and stalking respectively.

10. Similarly, in case of IT Act 2000 and its amendment in 2008, Section 66E, 67 & 67A have been inserted to make specific provisions for cyber crimes including those against Women,

Section 66E provides for punishment if someone "intentionally a knowingly captures, publishes or transmit the image of a private area of any person without his or her consent". The explanatory section defines 'capture', 'transmit' and 'provide area' for purposes of this Act. Section 67 provides for punishment for publishing or transmitting 'obscene material' in electronic form while Section 67A provides for publishing as transmitting 'sexual explicit content.' These provisions are under the category of 'computer related offences' and are gender neutral and not specific to cyber crimes against women. The scope of provisions is however not limited to 'computers' as the term 'communication device', has been defined as cell phones, personal digital assistance' or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

11. Dichotomy is noted in various provisions under IPC and IT Act in so far as punishment of cyber crimes is concerned. For example Section 67 and 67A provides punishment for publishing, transmitting of 'obscene material' and material containing sexually explicit act respectively, parallel provisions are available for such crimes in IPC under Section 292 and 294, which relates to selling, distributing any obscene material/object. However quantum of punishment in the two legislations for similar crimes is altogether different. IT Act provides for 5 year imprisonment and fine upto Rs.10.00 lakhs in the first convictism whereas IPC provides for imprisonment upto 2 years with fine upto 2,000/- in the first event.

12. Similarly, Section 66E of IT Act that caters to violation of privacy by way of capturing, transmitting image of any private area of any person without his/her consent is punishable with 3 years imprisonment and fine upto Rs. 2.00 lakhs. The corresponding provisions in Section 509 of the IPC which is gender specific for women and deals with similar crime of intruding upon privacy and to insult the modesty of women provide for imprisonment upto 1 year or with fine or both.

13. The dichotomy in the penal provisions for similar violations has been affecting the prosecution in cases of cyber crimes against women. It is in this context that Hon'ble Supreme Court in the case of Sharad Babu Digumarti vs. NCT of Delhi opined that in offences involving an electronic record, provisions of only IT Act would apply on the settled principle of law that special law would prevail over general laws and that the latter laws would prevail over prior legislations. This, however, raised another issue that similar crime is being treated differently on the ground of medium used for the crime. Moreover in many cases online and off line actions are mixed to commit the crime.

14. The general criticism against inadequacies of the two Acts lacking sensitivity to deal with cases of Cyber Crime against women are as under:

(i) Verbal harassment and abuses that do not contain sexually explicit contents are generally ignored by law enforcement agencies;

(ii) Criminal intimidation against women at the best cover personal threats, but do not address generalized and misogynistic abuses and systemic nature of such acts which are directed against a women because she is a women is often ignored;

(iii) Privacy is narrowly defined in term of physical privacy and conveniently ignores the informational privacy, and is largely viewed from the point of view of curbing obscenity or protecting the modesty of the women. Thus gender based psychological violence against women remains outside the domain of two laws;

(iv) Technology mediated forms of domestic violence within the home and by intimate partner relations also often gets ignored.

15. It has been felt in many quarters that the existing laws to curb cyber crimes against women are not adequate to cope with existing ground realities and a need has been felt that the legislation needs to take into account the exact social realities and need to be reformulated to facilitate provisions defining cyber crime in specific terms and provide for specific punishment for each crime.

16. The existing laws also need to be effectively enforced. Data about arrests on registered complaints of cyber crimes and rate of conviction in such cases is not available to have a conclusive view on the effectiveness of the existing legislations.

Other Issues with IT Act:

17. Some of the major issues that emerges, as a consequence of implementation of IT Act are as follows:

(i) Provision under 66A of IT act, punishing person sending reference message is very broad in nature and has the potential of encroaching upon the provision 19(1) (a) of the Constitution if annoyance, inconvenience or offensive instead of decency, morality or public order become the reason for invoking the provision of 66A, if would come in conflict with the right of freedom of speech.

(ii) Provision under Section 69A, granting powers to Central Government to block any public access to any information through a computer source is also very sweeping and cannot be judiciously applied in the absence of any elaborate guidelines. This has resulted in a situation where either there is no restriction or restriction if applied is subject to judicial scrutiny on the ground of being irresponsible.

(iii) Information Technology (Procedure and Safeguard for Blocking for access of Information by Public) Rule 2009, notified by Central Government under 69(A) (2) of the IT Act makes a provision for appointing a designated officer for the purpose of issuing direction for blocking the access by the public for any information, if needs approval of the review committee constituted under rule 149A of Indian Telegraph Rules 1951. Moreover, the request for blocking is to made by the nodal officers of an organization, which is restricted to (i) Ministries/Departments of Central Government (ii) State

Government/UTs (iii) any agency notified by Central Government. Whereas in case of individual requests, if can be send only with the approval of the chief secretary of concerned state. The process seems to be cumbersome. In this context the role of intermediate platforms on social media has also become important.

Cyber Security Policy, 2013

18. Ministry of Electronics and Information Technology pronounces the vision of the policy to "build a Secure Cyber Space for citizens, businessman and Government". The mission statement of the Policy inter-alia includes building of capabilities to prevent and respond to Cyber threats. Again the objective in the policy document refers in a general way about secure cyber, eco-system and to strengthen the regulatory frame work for this purpose. It refers to 'prevention, investigation and prosecution of Cyber Crimes and enhancement of law enforcement capabilities through appropriate legislative interventions. It also refers to create a culture of Cyber Security and privacy enabling responsible user behavior…" The policy is however, devoid of any reference to cyber crimes against Women and the sensibilities needed to curb the menace, which has a cascading affect on the Society at large.

Cyber Safety of Women:

19. Keeping in view the increasing number of women/ girls in the Cyber space, particularly in the age group of 18-24, and their vulnerability to severe harassment and exploitation, the legislative and law enforcement arrangements needed to deal with those taking advantage is not enough. It is equally important that women themselves are mindful of the danger, they need to be educated to become conscious of the ramifications and made well-equipped to take adequate preventive measure. Security precautions are necessary for any woman to protect herself from the menace of cyber crime are disseminated by various Institutions, particularly the cyber security cell of the Central Government and State Government. Government of India has also taken following steps to ensure safety of women from Cyber Crime:

1. **National Cyber Crime Reporting Portal:** The portal is managed by Ministry of Home Affairs. It has a separate channel for reporting crime against women/child related crime and reports can be filed in an anonymous manner or in a formal manner with a facility to track the action taken. The complaints filed are dealt by law enforcing agencies/ police.
2. **Cyber Crime Prevention against Women and Children Scheme**: Ministry of Home Affairs is implementing the scheme to handle the issues and develop facilities to check cyber crimes against women. The scheme has component of (a) online reporting unit (b) forensic unit (c) capacity building unit (d) R&D unit and (c) awareness creation unit. In addition to developing different units at Central level, Grant is also provided to States/ UTs for similar development and activities and for setting up of Cyber Forensic Training Lab, Training of police, prosecutors and judicial officers etc.

Moreover, a large number of civil society organization and NGO are working to protect women from Cyber Crimes by way of educating them, supporting them and even taking up their cases further.

Conclusion:

20. Availability of adequate cyber laws for cyber crimes against women, making them more specific with reference to the actual nature of such crimes in the society along with effective implementation of laws is essential to prevent the menace. Equally important is to educate women and girls about nature of cyber crimes and the latest technology, safety measures including privacy setting, needed to protect them and deal with such crimes. This would be necessary to encourage women to avail more cyber space and effectively participate in digital media. The nature of cyber crime may not be essentially directed towards any individual women but often it is misogynic in nature to discourage women to express themselves and articulate their social and political views in the cyber space. Free access to cyber space, an important human right of women needs to be protected by all means. For this purpose, the effectiveness of the legal provisions, law enforcing agencies, schemes to strengthen cyber security environment and institutional built up for the purpose, educating women and girls in cyber security and empowering them socially to raise their voice with the help of Civil Society Organization/ NGO are equally important. The present webinar proposed by the Commission, therefore, proposes to discuss the subject with specific reference to following two aspects:

A. **Cyber crime against woman-- Inadequacies of law or its ineffective implementation**.
B. **Making cyberspace safe for women-- Measures other than legal/ law enforcement**.

Two separate sessions with four speakers and one moderator/ speaker is proposed to be held for one hour each in the proposed webinar.

Bibliography

1. Ms. Sumaya Uma- 'Outlawing Cyber Crimes against Women in India'. Bharti Law Review April-June, 2019
2. IT for change- 'Technology mediated Violence against Women in India'- A discussion paper from IT for change Jan 2017.
3. Mansi Pukhraj Agarwal- 'Cyber Crime: Women Combating with the Negative effect of Technology in the Era of Globalization'- International Journal of Management and Humanities March, 2020

****