Available online at www.elixirpublishers.com (Elixir International Journal)

International Law

Elixir Inter. Law 65 (2013) 19673-19675

ISSN: 2229-712X

Cyber crime against women and the Law: an analysis

Siddharth Mehta
Amity Law School, IP University. Delhi.

ARTICLE INFO

Article history:
Received: 3 October 2013;
Received in revised form:
25 November 2013;
Accepted: 3 December 2013;

Keywords
Cyber crime,
Women,
Authorities,
Provision.

ABSTRACT

In 2000, an MMS Scandal featuring a minor girl from a South Delhi Public School performing oral sex on her classmate was leaked online. The clip was reportedly put up without the girl's consent. The scandal started a dangerous trend of video recording of intimate moments and uploading them on the Internet due to the monetary benefits associated with it or the 'kick' derived by a jilted Male partner in tarnishing the reputation of the female participant. The IT Law which was in its nascent stage at that time showed its total inability to counter this problem. A decade hence and after a comprehensive amendment to the statute, the Cyber Law in India still shows an eerie inability to prevent or punish such acts. Apart from this, women in the cyberspace are vulnerable to a variety of crimes such as Identity theft, Cyber Morphing, Obscene messaging, Cyber Defamation etc. Usually, the victim has little or no recourse against the criminal since such crimes are committed anonymously. This coupled with an untrained police, onerous enforcement mechanism, and lack of technology to undo the cyber attack and most importantly the stigma associated with the event leaves Women disempowered in the Cyber Space. Also, the patriarchal setup of the society sees them as a willing participant rather than a victim to the crime. The Anara Gupta Sex Scandal Case is one classic example of how difficult it is for a victim of Cyber Crimes to get justice in India. Against the foregoing backdrop, the paper will analyze some pertinent loopholes in the Cyber Law in India. The paper also attempts to suggest some structural reforms apart from the amendments in the substantive Law which need to be incorporated to improve the situation which is otherwise grim.

Introduction

Cyber Crime of Obscenity Against Women: Meaning and Scope

Cyber Pornography has been a highly debated issue in India. While some activist groups have vociferously fought for banning of blocking of Pornography Websites in India, any interference of the government in this regard is usually seen as a 'regressive' step. The controversy that followed the blocking of the popular "Savita bhabhi" website is one example how pornography is being defended on the grounds of freedom of speech and expression.[1]

However, amidst these two viewpoints what is generally ignored is that a lot of women in India, unknowingly fall victim to instances of leaked clips of sexual intercourse or cyber morphing which depicts them in poor light. These gruesome acts violate the privacy as well as dignity of the women.

There have been innumerable instances where videos of sexual intercourse between the women and her partner are cleverly made by using a spy camera often without the permission of the women. Often, the videos are leaked either to prove a point against that women or if she refuses to the keep a relationship with her partner. [2]

Also, at times spy cameras are cleverly hidden in hotels, public bathrooms, changing rooms of shopping malls etc. The tape acquired from such cameras is usually sold to the underground pornography industry for earning money or is uploaded on the Internet for some misguided adventure. The indelible scar that such actions leave on the psyche of the concerned women are often not taken into consideration by such perpetrators. These acts have proven to be such a menace that even Bollywood actresses have fallen victim to this crime[3]. Usually, such a practice takes place with the connivance of the staff, but it seldom gets detected. The recent case of leaking of footage of couples getting 'cozy' in the Delhi Metro is one example of how anynonymously such crimes can be carried out.[4]What is more puzzling is that the 'victim blaming syndrome' again came into play in this case and no attempt was made by the concerned authority to make an attempt to find out the perpetrators responsible for such a ghastly assault.

[1] Hemraj Singh, "*Pornography Law : Savita Bhabhi Must Go*" ,Lawyer's Update, April 2010

[2] Nishant Shah, *"Playblog: Pornography, Performance, and Cyberspace"- Centre for Internet and Society.* Available at http://cis-india.org/publications-automated/cis/nishant/playblog%20performance%20pornography%20cyberspace.pdf/view Last accessed August 2 2013 , 7:45 PM

[3] Ibid

[4] Recently, over 250 Clips of couples 'making out' in the Delhi Metro premises were leaked on various porn sites. The scandal could not have happened without the connivance of the staff. The DMRC has ordered an 'inquiry'. http://www.indianexpress.com/news/stung-by-porngate-delhi-metro-urges-passengers-to-behave/1145561/ Last accessed August 2 2013, 8:00 PM

Tele:
E-mail addresses: siddharthlaw19@gmail.com

Recently, there have also been a spate in India of instance where rape victims were filmed in the Act and the video was circulated on the Internet or at times the video was used as a shield by the rapists to prevent the victim from reporting the incident. This incident goes on to show the level to which this technology can affect the lives of the people and how it can interfere with the criminal justice system in India.

Cyber Crimes Against Women And The Loopholes In The Law

Sections 66E, 67 and 67A deal with the offences of Violation of Privacy, publishing of obscene material in electronic form and publishing of sexually explicit act in electronic form. At the first glance, the provisions seem to provide enough deterrence for such acts, however, on a closer analysis it becomes clear that there are a lot of loopholes in these provisions which are liable to be used during the trial stage. Section 66E punishes a perpetrator who "intentionally or knowingly captures or transmits the image of the private area of a person without his or her consent, under circumstances violating the privacy of that person". However, a careful perusal of this section makes it clear that "morphing" the image of the person over the naked or scantily clad image of another person wouldn't constitute a crime under this provision. Thus, for instance if a person copies the image of a girl from a social networking website, morphs it on a naked image (which is not captured by him), he would not be liable under this provision. He can only be booked for Outraging the Modesty of a woman under Section 354 IPC or for defamation under Section 499. Now, prosecution under these provisions would be a great travesty of justice in as much as the maximum punishment under these Sections is highly incommensurate with the mental trauma caused to the victim. A perpetrator can virtually cause the "social death" of a person and yet receive a very lenient punishment for that.

Also, the enforcement mechanism of these provisions doesn't seem to be in harmony with the substantive law at all.

The Information Technology Act, 2000 envisages a very dilatory mechanism for dealing with such offences. According to the Information Technology Intermediary (Guidelines) Rules, 2011, every intermediary is required to assist the person against whom a cyber offence has been committed within 36 hours to disable the information.[5] Also, the Intermediary is required to provide the name and contact details of the grievance officer who is obliged to look after the complaints of users in relation to cyber offences. The officer is required to completely dispose off the complaint within one month from the date of receipt of the complaint.[6] The issue that merits consideration is whether the period of 3 days is reasonable especially when information can be shared at lightning speed throughout the world via the Internet and there is a possibility that in three days time, the offending content may be accessed by a large number of people leaving the victim of such an offence without any recourse?

Further, would it be enough to have one grievance officer for an Intermediary of a huge nature such as Facebook, Twitter, Orkut etc which manages Millions of Users in India alone? Moreover, social networking websites such as Facebook, Twitter etc. are yet to comply with Rule 3 of the aforesaid rules. There is no information pertaining to the Grievance Officer available on these websites. In such a case, most of the women have no recourse against their perpetrator. Even if a Police Complaint is lodged by the victim, the time taken to remove the objectionable content will be too much. Again, in cases of cyber morphing or identity theft, the only way the victim seeks to address is it by using the 'report' feature available on such websites and by asking their friends to do the same. Often, it is noted that these websites are reluctant to remove content and it usually requires a court order to compel them to remove the offensive content.

According to The Information Technology (Procedure and Safeguards for Blocking for Access of Information By Public) Rules, 2009, the request for blocking of information under Section 69A of the IT Act has to come either through the joint secretary or through the nodal officer of an organization[7]. If a complaint were to proceed from a private person it has to first get the approval of the Chief Secretary. [8] The designated officer is not allowed to take a complaint directly from any person. [9] The designated officer is not permitted to deviate from this rule even in the case of emergency.[10] Further, on receipt of the complaint, the designated officer is required to forward it to a committee consisting of himself and officers not below the rank of Joint Secretary in Ministry of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Emergency Response Team.[11] After, the examination of request a notice is to be issued to the concerned person against whom a complaint is made for his representation and at least 48 hours have to be given to him to appear before the committee.[12]

Although, Rule 9 makes an exception to this procedure and provides that the designated officer may in "any case of an emergency nature" submit the request to the Secretary, Department of Information Technology, who may if he satisfied order the blocking of the material without giving an opportunity of hearing to the person against whom a complaint has been made[13] No explanation has been provided to clarify the meaning of the said

Rule 11 provides that the complaint received from a Nodal Officer has to be disposed off as "expeditiously as possible" and in no case beyond a period of seven days.

Again, the question arises with regard to the time taken to block content which is a week in this case.

The Ministerial Order on Blocking of Websites, 2003 recognizes the need for blocking websites. It lays down

"The Blocking of website may be the need of the several agencies engaged in different walks of public and administrative lives due to a variety of reasons. Explicit provision for blocking of the website in the IT Act is available only in Section 67 relating to pornographic content on the website. In addition, section 69 empowers the Controller of Certifying Authorities to intercept any information transmitted through any computer resource in relation ....."[14]

It further lays down

"*As already noted there is no explicit provision in the I.T. Act, 2000 for blocking of websites. In fact, blocking is taken to amount to censorship….But websites promoting hate content,*

[5] Rule 3, IT (Intermediary Guidelines), Rules 2011

[6] Rule11, IT (Intermediary Guidelines), Rules 2011

[7] Rule 1

[8] Proviso to Rule 6

[9] Rule 6(3)

[10] Rule 9

[11] Rule7

[12] Rule 8

[13] Rule 9(2)

[14] Para II, Ministerial Order on Blocking Of Websites Vide G.S.R. 529(E) dated 7th July, 2003

slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech… Blocking of such websites may be equated to "balanced flow of information" and not censorship"[15]

It provides that the complaint can be addressed to the Director, CERT-In for blocking of a website. However, the list of officers through which the complaint can be sent is very limited. Thus, in respect of the Police, only the Director General of Police can make such a complaint.[16]

There is no provision for the aggrieved person to make the complaint himself. Further, the complaint again has to go through the rigours of screening through a committee which will take at least one day to decide whether the website is required to be blocked or not[17]. Also, it must be noted that in order for a complaint to reach the DGP and from there on to the CERT would take a long time, thus making the remedy useless for the victim.

Also, it is pretty well known that it is difficult to get an FIR registered in India, for which the Code of Criminal Procedure contains an alternate complaint mechanism under which a complaint can be made to the Magistrate for inquiring into a cognizable offence in which the FIR is not being registered.[18] It is doubtful whether such a system would be appropriate in dealing with offences of such a nature which need to be dealt with urgently and sensitively. The last resort left with the victim in such a case would be to approach the court for removal of such offensive content; however, this remedy will not come without uncalled for publicity.

Other challenges for authorities in dealing with cyber crime against women

Cyber Law experts have been often been very vocal about the fact that the majority of the Police Officers in India are not equipped with even the basic knowledge of Information Technology, in such a case it is difficult to expect that the investigation conducted by them would bear any fruit. Often, they are not clear about collection of Digital Evidence and matters of a like nature. There are only four cyber cells in the Metropolitan Areas right now. Further, unlike the Economic Offences Wing there is no special wing to deal with pornography and morphing relating crimes against women. Thus, the level of sensitivity and sophistication with which such complaints are required to be handled is missing in the current policing system in India

Also, there is only one Forensic Laboratory in Hyderabad which serves the whole of India when it comes to dealing with cases of Cyber Crimes[19]

It has also been observed that the Lower Judiciary in India is not quite Cyber Savvy and hence is not equipped to view Cyber Crimes with the sensitivity with which these crimes are normally required to be viewed. There is a need to provide frequent training to the officials at these levels to help them to understand the modus operandi, implications etc of such crimes. The speed with which this technology is developing requires even experts to receive frequent training on these aspects.

Also, attempts are required to be maintained between different countries to coordinate efforts for cyber security, so that the transnational cases can also be dealt with quickly.

Conclusion

The Central Government last year ordered the social networking websites to pre- screen the content before posting it on the website[20]. The order met with huge opposition from the civil society activists because it was widely perceived as an attempt on the part of the government to curb dissent[21]. However, the author takes the view that in the case of pornography or content of obscene nature which can be objectively assessed, the pre screening should be done. Other material such as religious criticism etc. may not be pre screened and may be subjected to the existing mechanism. As far as Pornography is concerned it is clear that the Social Networking websites are not only prohibited from hosting such content but are under an obligation from preventing such content against other users from being uploaded[22], thus even if the social networking websites are allowed to pre screen such content it is not likely to cause any issues. For such purpose, the definition of obscene content as laid down under Section 66E and Section 67 can be taken as a reference point, so that no content is arbitrarily prevented from being posted.

Also, the response mechanism for blocking websites needs to be swift so that before such information can be shared it is removed and the social image of the victim remains protected. New regulations need to be drafted by the government in this regard.In view of the increasing cyber crimes it is also necessary to increase the bench strength of the various authorities required to deal with cyber crimes under this Act. Conditioning of people at various levels is also required in order to sensitize them that the victim of a cyber crime is not responsible for it.

[15] Para III, ibid
[16] Para V, sub Para 1 , ibid
[17] Para V, sub Para 2, ibid
[18] Section 156(3), CrPC

[19] Karnika Seth, "*Evolving Strategies for the Enforcement of Cyber Laws"* available at http://www.karnikaseth.com/evolving-strategies-for-the-enforcement-of-cyberlaws.html Last Accessed on August 4, 2013 8: 30 PM
[20] Available at http://india.blogs.nytimes.com/2011/12/05/india-asks-google-facebook-others-to-screen-user-content/?_r=0
[21] ibid
[22] Rule 3 of the IT (Intermediary Guidelines) Rules, 2011