Cyber Stalking In The Indian Scenario And The Indian Information Technology Act, 2008.

Dr.Mrs.Hema.V.Menon*[1]
Assistant Professor,
Dr.Ambedkar College,
Deekshabhoomi,
Nagpur,Maharashtra.

Abstract

The progression of society, and the expansion of the Internet in this millennium have brought to fore a new medium for abuse, namely cyber stalking. It is of such horrific magnitudes that without revealing the identity or physically meeting the victim a perpetrator can cause severe trauma to the victim. The very nature of this kind of online crime is such that the police or the victim have very little information regarding the harassers, as most victims either don't know their harasser or do not know enough information about them for the police to record and apprehend the perpetrator. Cyber stalking is a criminal offense under the laws of many countries including India. Section 66A of the Information Technology Act, 2000 as amended by the Amendment Act of 2008 recognised cyber stalking as a crime for the first time. The Criminal Law (Amendment) Bill, 2013, India is recognises that stalking includes monitoring of a person's use of internet, email and electronic communication. This research paper studies ingredients of cyber stalking as a crime, Indian Law vis a vis cyber stalking and few reported and unreported cases with respect to it. The pur[ose of this paper is to highlight the Indian legal system with respect to cyber stalking. The objective of the research thereby is to study the legislative perspective of cyber stalking .

Key Words: Cyber stalking, Ingredients of cyber stalking, Information Technology Act

Introduction

The world of computers and communications implies today's fast-moving, high technology world.iCyberspace is dynamic, undefined and exponential. The IT revolution has resulted in an unprecedented increase in the number of Internet users.It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education. However, Internet also has it's own disadvantages namely it has also given rise to new and unique forms of crimes which are the illegal activities committed on the Internet. These can be broadly termed as cyber crimes. Such activities intrude into our privacy, economic and social life alike which is as traumatic and harmful as the physical crimes.Some scholars have

interestingly argued that, “in the Internet nobody knows you are a dog”ii.Computer crimes or cyber crimes as they are called have have increased manifold and cyber stalking is one of them and also is considered the most dangerous. Cyber stalking is the use of the Internet, email or other electronic communications to stalk, and generally refers to a pattern of threatening or malicious behaviors.

Stalking

The dictionary meaning of the adjective ‘stalking’ means “of or relating to the act of pursuing or harassing” The word stalking was not commonly known until various instances happened. The legal definition of stalking varies from country to country. Various definitions are available in several books, out of which it can be stated that the common elements are;

- Repeated and unwanted behaviour whereby one individual attempts to contact another individual, and
- The behaviour causes the victim to feel threatened or harassed.

Stalking has become a greater problem to women and children in comparison to men. The victim is normally a person who is less thorough regarding internet services and its applications. The stalker is generally a person who is a paranoid with no self-esteem. But the traits differ from one stalker to another. Some harass to seek revenge or some do so for their own pleasure. While some just do it for playing mischief.iii

Cyber Stalking

There is no universally accepted definition of cyber Stalking, but accordfing to Bocjj,it is generally defined as iv "A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology to harass another individual, group of individuals or organisation. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, damage to data or equipment, identity theft, data theft, computer monitoring, the solicitation of minors for sexual purposes and any form of aggression. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress."

Cyber stalking is a technologically based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyber stalking can take many forms, including:

1. Harassment, embarrassment and humiliation of the victim
2. Emptying bank accounts or other economic control such as ruining the victim's credit score

3. Harassing family, friends and employers to isolate the victim
4. Scare tactics to instill fear and more

Two Different Kinds Of Cyber Stalking Situations That Can Occur:

1. Online harassment & cyber stalking that occurs & continues on the Internet.

2. Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address.v

The typical areas where the stalking takes place are;

1. Live chat rooms/flaming
2. E-mail,

Discussion forums and;

Message boards.

3. Open publishing websites (e.g. blogs and Indy media)

There are three primary ways in which cyber stalking is conducted (Ogilvie, 2000)

- Email Stalking: Direct communication through email.
- Internet Stalking: Global communication through the Internet.
- Computer Stalking: Unauthorised control of another person's computer.

Information Technology Act, 2008 (ITA 2008)

Section 66A of the Information Technology Act, 2008 (ITA 2008) states, "Punishment for sending offensive messages through communication service, etc:

Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITA 2008) shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer,

computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message."

The aforesaid section creates an onus on the sender of the message by means of a computer resource (section 2(1)(k)) or a communication device (section 2(1)(ha)),which may be:

(a) grossly offensive or menacing in character; or
(b) known to be false, but is being sent purposefully and persistently to cause s
(c) cause annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.(by stripping headers and footers details from emails to avoid detection; spoofing IP address etc.)

Such messages can be in the form of text (emails, SMSes, Blogs, Vblogs, Tweets), image, sound, voice (VoIP-Voce over internet telephone services like gTalk, Skype) etc. However, it is to be seen from the recipient's perspective about the nature of harm caused to him by the sender's message(s).

Nature of message sent	Nature of offence(s)
(a) The message was grossly offensive or menacing in character.	Obscenity in electronic form, morphing (of images) defamation, text bullying, stalking etc.
(b) The message is known to be false, nevertheless sent, caused annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.	Criminal intimidation, extortion, public mischief, morphing (of images), insult, threat to cause injury, stalking etc.
The message caused annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.	Spamming, unsolicited emails/telephone calls etc.

(Table depicts nature of offence resulting from the nature of message sent.)

Incidents like texting (sending persistent text messages) and sexting (sending sexually explicit photographs/MMS) have emerged in the recent past as major cyber offences. Both texting and sexting are covered under this section.

Offences under section 66A are punishable with imprisonment for a term, which may extend to three years and with fine.vi

Criminal liability in India for cyber crimes is defined under the Indian Penal Code (IPC). Following sections of IPC deal with the various cyber crimes:

- Sending threatening messages by e-mail (Sec .503 IPC)
- Word, gesture or act intended to insult the modesty of a woman (Sec.509 IPC)
- Punishment for criminal intimidation (Sec.506 IPC)
- Criminal intimidation by an anonymous communication (Sec.507 IPC)
- Obscenity (Sec. 292 IPC)
- Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail (Sec.292A IPC)
- Obscene acts and songs (Sec.294 IPC)

In India there are number of cases filed under these IPC provisions related to the cyber crime. According to the report of Home Ministry, in 2012 there are 601 cases filed under the various provisions of IPC.vii

Some of the functioning Government reporting agencies in India are:

1. cybercrime@kolkatapolice.gov.in
2. http://www.cyberpolicebangalore.nic.in/
3. cbcyber@tn.nic.in
4. http://www.cybercellmumbai.com/
5. http://www.cyberkeralam.in
6. http://www.punepolice.com/crime_branch.html
7. http://www.thanepolice.org

Jurisdiction:

Territorial limitation on the Internet becomes of peripheral nature in the virtual medium as the web pages on the net can reach almost every province in the nation and conceivably almost every nation on the globe. This is where the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world.The IT Act will apply to the whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. However, if a crime is committed on a computer or computer network in India by a person resident outside India, then can the Courts in India try the offence? According to Sec.1 (2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further, Sec.75 of the IT Act, 2000 also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence or contravention committed

outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Conclusion:

The Information technology age has become a boon to the human community, but this paradigm-shift is also reflected in the area of crime, as along with the positives there is a wide spectrum of negatives which has become a cause of worry because the negative facets are being efficiently utilized by the sadistic minds of the society for committing crimes in the virtual environment called the Cyber Crimes.

In 2011, six young ladies in Coimbatore filed a complaint with the Cyber Cell of the Police Department, alleging that they were receiving menacing calls repeatedly from an unidentified number. Investigations traced the call to a single person making similar calls to various other young ladies repeatedly. Although hundreds of ladies were reportedly victims, only a few came forward to complain to the police. The police arrested the person under Sec 66A of IT Act and got him convicted in 2014 to one year of imprisonment. He is in prison now.

Noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal said that, "While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cyber crime friendly legislation; – a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law;.. a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world……" viii

Suggestions:

- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.
- Strict statutory laws need to be passed by the Legislature keeping in mind the interest of netizens (cybercitizen or an entity or person actively involved in online communities and a user of the Internet).
- There is a need for a well-equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime

cells in all metropolitan and other important cities. Further the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI).

---

[i] Read more at http://www.yourdictionary.com/cyberworld

[ii] Christopher Reed,Internet Law; Text and Materials, 2000 at page 119

[iii] http://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/

[iv] Bocjj Paul (2003). Victims of cyber stalking: An exploratory study of harassment perpetrated via the Internet First Monday, volume 8, number 10 (October 2003),
URL: http://firstmonday.org/issues/issue8_10/bocij/index.html

[v] ibid

[vi] Vakul Sharma,Information Technology-Law and Practice,3rd Edn.(New Delhi:Universal Law Publishing Co Pvt.Ltd.,2011).

[vii] http://www.mha.nic.in accessed on 4th Dec 2013

[viii] Pawan Duggal, Is this treaty a treat? Available at http://www.naavi.org/pati/pati_cybercrimes_dec03.htm