CYBERCRIMES AGAINST WOMEN IN INDIA

Written by ***Shefali Singh***

Lawyer

INTRODUCTION

With the introduction of internet, the lifestyle of people has become very convenient as there is not much effort required so as to make a search or to place an order or to share news to public at large. Today it is quite possible for an individual to spread a word with a click of button on computer. People have become a slave of such invention as they blindly trust the information so being provided without checking for its authenticity. Hence, it has become a platform for some to use it for all the wrong purposes. With an increase in the crime rate committed online at the cyberspace, a need was felt for a legislation to regulate such crimes. For the first time, a Model Law on E-commerce was adopted in 1996 by United Nations Commission on International Trade and Law (UNCITRAL). It was further adopted by the General Assembly of the United Nations by passing a resolution on 31st January, 1997. Further, India was also a signatory to this Model Law and had to revise its national laws as per the said model law. Therefore, India enacted the Information Technology Act, 2000[1].

Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records i.e. the data what is stored in a computer or an external storage attached thereto[2].

[1] Available at http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/16/16_chapter%207.pdf last accessed on 02 October 2017.
[2] Available at http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf last accessed on 02 October 2017.

The culprits got out of the hands of law as with the rise in the new crime like voyeurism were not covered under the Act. The increasing need for legislation was felt which covered like crimes which led to amendment in the year 2008. In the year 2013, Criminal Amendment was introduced which covered the crimes against women which could not earlier covered under the Information Technology Act, 2000.

Even though India is one of the very few countries to enact IT Act 2000 to combat cybercrimes, violation of rights of women still remain untouched in this Act. The Act has defined certain terminology such as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. Crime against any person whether men or women is a crime against the society at large. Such an increase in the cybercrime is taking place due to increasing diffusion of the internet and economic expansion.

Some of the notable features of the ITAA, 2008 are as follows:

i. Focusing on data privacy
ii. Focusing on Information Security
iii. Defining cyber café
iv. Making digital signature technology neutral
v. Defining reasonable security practices to be followed by corporate
vi. Redefining the role of intermediaries
vii. Recognising the role of Indian Computer Emergency Response Team
viii. Inclusion of some additional cybercrimes like child pornography and cyber terrorism
ix. Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)[3]

The researcher has followed the following method so as to have in depth knowledge with respect to the crimes against women arising at cyberspace-

CONCEPTUAL UNDERSTANDING OF CYBERCRIMES

The concept of cybercrime is not radically different from the concept of conventional crimes both include conduct whether act or omission. It follows same principle and it also need to have

[3] *Supra* Note 4.

two elements to become cybercrime as conventional crimes i.e. *actus reus and mens rea*.[4] Cybercrime is an evil having its origin in the growing dependence computers in modern life. Everything is mix of positive and negative sides, so is the Internet. For all the good it does us cyberspace has its dark sides too. Unlike conventional communities though, there are no policemen is patrolling the information superhighway, leaving it open to everything from Trojan horses and viruses to cyber stalking, trademark counterfeiting and cyber terrorism. The problem is multi fold as it covers crime related to economy as well as other crimes against morals standards which use parameters like indecency and obscenity.

Definition of Cybercrime:

Cybercrime is a generic term that refers to all criminal activities done using the medium of communication devices computers, mobile phones, tablets etc., the Internet, cyber space and the worldwide web. It can be said that cybercrime is species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.

This term "cybercrime" has nowhere been defined in the statute (Information Technology Act, 2000) passed or enacted by the Indian Parliament. A generalized definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both." The simplest and one among the first official definition given by group of experts constituted by OCED (Organization for Economic Co-operation and Development) in 1983. According to OCED the term computer crime means as any illegal, unethical or unauthorized behaviour involving automatic processing and transmission of data.[5]

Cybercrime consists of only those offences provided in the Information Technology Act, 2000. As per this definition, cybercrimes would mainly be restricted to tampering with the computer source code, hacking and cyber pornography. Cyber fraud, defamation, harassment, email abuse and IPR (Intellectual property rights) thefts etc., can be said to be acts of commission or omission committed on or through or with the Internet, whether directly or indirectly, which is prohibited by any law and for which punishment, monetary and/or corporal, is provided. Cyber Crimes can be classified as: -

[4] Yourdictionary.com, 'Cybercrime and The Coincidence Of Four Critical Elements Dictionary Definition | Cybercrime And The Coincidence Of Four Critical Elements Defined' (2015) available at http://www.yourdictionary.com/cybercrime-and-the-coincidence-of-four-critical-elements (last accessed on October 09, 2017).

[5] Clough J, Principles of Cybercrime (*Cambridge University Press* 2010).

i. Traditional crimes committed on or through the new medium of the internet. For example: Cheating, fraud, Misrepresentation, pornography, theft etc. committed on or through or with the help of the internet would fall under this category.
ii. New crimes created with the Internet itself such as hacking and spreading viruses etc.
iii. New crimes used for commission of old crimes. For example: where hacking is committed to carry out Cyber frauds.[6]

Characteristics of Cybercrimes:[7]

i. The weapon with which cybercrime are committed is technology. Cybercrimes are the work of technology and thus Cyber criminals are technocrats who have deep understanding of the Internet and computers.
ii. Cybercrime is extremely efficient i.e. it takes place in real time. It may take seconds or a few minutes to hack websites or do cyber frauds.
iii. Cybercrime knows no geographical limitations, boundaries or distances. A cybercriminal in the one corner of the world can commit hacking on a system in the other corner of the world. For example: a hacker in the US can in real time hack in the system placed in Japan.
iv. The act of cybercrime takes place in cyberspace which makes the cybercriminal being physically outside cyberspace. All the components of cyber criminality from preparation to execution, take place in the cyberspace.
v. Cybercrime has the potential of causing harm and injury which is of an unimaginable magnitude. It can easily destroy websites created and maintained with huge investments or hack into websites of Banks and the defense department's websites.
vi. Due to anonymity and invisibility of cyber criminals and its potential to affect in several countries at same time, which are different from the place of operation, it is extremely difficult to collect evidence of cybercrime.

Evolution of Cybercrimes:

The process of criminalization of the human behaviour judged to be harmful to the public is typically one that builds slowly in common law jurisdictions. Momentum gained through

[6] *Id.*
[7] Ojp.gov, 'Internet Crimes Against Children' (2016) available at http://ojp.gov/ovc/publications/bulletins/internet_2_2001/internet_2_01_5.html (last accessed October 09, 2017).

problem identification and pressure exerted by special interest groups which can easily take decades before undesirable actions are classified as "crime". In some instances, this process is accelerated through the occurrence of certain "catalyst events" that captures the attention of the public and the attention of lawmakers[8].

In the case of computer crime, legislators grew increasingly attentive in the 1980s as businesses became more dependent upon computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations.

Although, the first cybercrime took place back in 1820, when a textile manufacturer in France who produced the loom with a device which allowed the repetition of a series of steps in the weaving of special fabrics. This device became a threat for the employees' employment and livelihood and they discouraged the manufacturer from using the new technology by doing acts of sabotage.[9]

Later in modern times, first cybercrime started out as hackers who breaks into computer networks. Some of them used to break into high-level security networks just for kick out of it, but others used to gain sensitive, classified material. Eventually, criminals started criminal activities which are traditional in nature, such as theft, fraud, forgery, defamation and mischief to with the computer by spreading viruses onto other computer systems. Next came the problem of phishing scams and credit card theft and subsequently, identity theft became prevalent among cybercrime.

CYBERCRIMES AGAINST WOMEN IN INDIA

Women are being attacked online with threats of assault, rape and murder, particularly when identifying locating information is attached, are not safe in their homes, neighbourhoods and workplaces. Emotional and psychic harms are pervasive and penetrating: a woman or girl is robbed of her self-possession, her security in her own body, her self-esteem, her peace of mind, and essentially her comfort in her world; she is alienated from her own sexuality, which becomes a source of anxiety and threat; she feels her future slipping away and out of her control; she loses her sense of oneness with other human beings, either in community,

[8] *Id*
[9] Latta S, *Cybercrime* (Enslow Publishers 2012)

neighbourhood, workplace, as the "other" becomes a source of threat and harm rather than nurturance and support[10].

Since such crimes are on a rise it is necessary to critically study the various types of crimes taking place in cyberspace. Following are the various cybercrimes taking place related to women in India: -

Hacking-

Hacking is a generic terminology used in the world of computers whose origin is traced by Jargon Dictionary which means one who makes furniture with an axe and the term was used for the first time in computer world in 1960's. It means unauthorized access to a computer system. This unauthorised access can be to any programmes or data stored in the computer. It is the most common type of cybercrime being committed across the world.

There are two types of hackers generally:

i. The amateur group who are obsessed with internet and does it for fun or hobby or gain knowledge about actual working of computer, they do not intent to involve into criminal activity;
ii. Hackers, who intent to engage in criminal activity by causing damaging the business of competitors or frauds or misappropriation.

The word 'hacking' has been defined in section 66 of the Information Technology Act, 2000 as follows:

"*Whosoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking.*"

Punishment for hacking under the above-mentioned section is imprisonment for three years or fine which may extend up to 2 lakh rupees or both.[11]

[10] Danielle Citron, Hate crimes in cyberspace, *Harvard university press* (2014)

[11]Sec. 66, Information Technology Act, 2000

Cyber Stalking-

Cyber stalking refers to the crime of using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person. Cyber stalking most often involves sending harassing emails, instant or text messages, or social media posts, or creating websites for the sole purpose of tormenting the victim. A cyber stalker acts of out of anger, or a need to control, or gain revenge over another person through threats, fear, and intimidation. There are several forms of cyber stalking, including:

i. Harassing the victim
ii. Embarrassing and humiliating the victim
iii. Exerting financial control by emptying the victim's bank accounts, or by ruining his credit
iv. Isolating the victim by harassing his family, friends, and employer
v. Frightening the victim by using scare tactics and threats[12].

While cyber-bullying and cyber-harassment may damage an individual's reputation or livelihood, cyber-stalking is more likely to result in severe and immediate emotional or physical harm. [13]

Harassment via E-mail-

Harassment via email is a form of harassment, which includes blackmailing, threatening, and constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box. Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cybercrime. After the amendment in 2008 new Sections have been inserted as Section 67 A to 67 C Section 67 A and 67 B insert penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe. These provisions do not mention anything about e-mail harassment of different type but in general they are used to book the perpetrators along with Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman. The issues related to

[12]Available at legaldictionary.net http://legaldictionary.net/cyberstalking/ (last accessed on October 17, 2017)
[13] Jacqueline D. Lipton, Cyber- Victimization, *ExpressO* (2010)

publication or transmission of obscene information in electronic form under Section 67 of IT Act 2000 may be looked from the perspective of 'extraterritorial' jurisdiction. With the advancement of technology that obscene is no longer a local phenomenon.[14]

Cyber sexual defamation-

Cyber sexual defamation happens between real or virtually known people who out of frustration start publishing defaming stories in obscene languages on various social websites subsequently it turns into cyber pornography. The accused can be booked under section 67 and 72 of the IT Act as well as IPC as discussed earlier.[15]

Cyber Pornography-

The growth of technology has flip side to it causing multiple problems in everyday life. Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly called as widespread. Almost 50% of the web Sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs.[16] The new technology is not merely an extension of the existing forms like text, photographs and images but full motion video clips are also available. Another great disadvantage with it media like this is its easy availability and accessibility to children who can now log on to pornographic websites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present. Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the Internet.[17]

Cyber flirting-

Generally cyber flirting may be considered very minimal petty offence that starts when perpetrator force the victim to hear obscene songs, messages and it may consequently result in cyber sexual defamation and breach of thrust. Again, this can be treated as the flip side of IT

[14] Shobhna Jeet, Cybercrimes against women in India: Information Technology Act, 2000, *Elixir Criminal Law* 47 (2012) 8891-8895
[15] Supra, note 9
[16]Bequai A, 'Prosecuting Cyber-Crimes' (1996) 1996 *Computer Audit Update*.
[17] Godwin M, *Cyber Rights* (MIT Press 2003).

Act that except Section 72 which deals with the breach of confidentiality and privacy there is no other support that can be offered by the Act to the victim.[18]

Cyber Bullying-

Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. The main aim and objective behind such crime may be to defame the target out of anger, hatred or frustration or secondly when the perpetrator wants to make simple fun of his friends, classmates, juniors or unknown net friends. The social network like Orkut, Facebook can be considered the main source of cyber bullying. But despite of the vulnerability of women net surfers IT Act does not provide some direct protection to the victims. While most of the crimes can be booked under IPC, under IT Act there are only three provisions which connote cybercrime i.e. Section 67, 70 and 72. It is true that, other than cyber stalking, cyber pornography and morphing, men are equally susceptible to the other types of crimes mentioned here. But the majority of the victims of such offences are women as can be seen from the above study. Despite of that there is no separate provision for cybercrimes against women under IT Act.[19]

Important Cases:

i. *Regina v Hicklin*[20]*:*

It is also known as Hicklin's test which is a legal test for obscenity established by UK. The court held that all material tending "to deprave and corrupt those whose minds are open to such immoral influences" was obscene, regardless of its artistic or literary merit. Later, in the case of United States v Ulysses[21] it was held that the test for obscenity was whether the publication considered as a whole is obscene and not if the content contains isolated obscene material.

ii. *Chandra Kant Kalyan Das v State of Maharashtra*[22]*:*

Supreme Court adopted the '*likely audience test'* unlike the '*the most vulnerable test*' in the Hicklin Test. It held that the term obscenity and its meaning vary from jurisdiction to jurisdiction based on the moral and cultural element of the contemporary society.

[18] *Supra* Note 13
[19] *Id*
[20] (1868) 3 QB 360
[21] 72 NY 705 (2nd Cir 1934)
[22] (1969) 2 SCC 687, AIR 1970 SC 1390

iii. K.A. Abbas v Union of India[23]*:*

The petitioner for the first time challenged the validity of censorship as violative of his fundamental right of speech and expression. The Supreme Court however observed that, pre-censorship of films under the Cinematograph Act was justified under Article 19(2) on the ground that films have to be treated separately from other forms of art and expression because a motion picture was able to stir up emotion more deeply and thus, classification of films between two categories 'A' (for adults only) and 'U' (for all) was brought about.

iv. Ajay Goswami v Union of India[24]*:*

Reader the court took a liberal view point and laid down 'responsible reader test' to judge obscenity. The court took the view that a complete ban on publishing news items or pictures will mean that newspapers will be publishing only child friendly content. This will deprive adults from reading entertainment materials that are 'permissible under the normal norms of decency in any society'.

AN ANALYSIS OF LEGAL FRAMEWORK IN INDIA

The IT Act was enacted in India and brought into effect on the 17th October, 2000. The Act extends to India and is also applicable to an offence or contravention which is committed by any person.[25] The object of the IT Act is crystal clear from its preamble which shows that it was created mainly for enhancing ecommerce hence it covers commercial or financial crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unaware about the safety of net users. Under the following sections majority of cybercrimes are being dealt:

I. Section 43- deals with penalties and compensation for damage to computer, computer system etc. This section is the first major and significant legislative step in India to combat the issue of data theft. The IT industry has for long been clamouring for a legislation in India to address the crime of data theft, just like physical theft or larceny of goods and commodities. This Section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in charge of a

[23] (1970) 2 SCC 780, AIR 1971 SC 481
[24] (2007) 1 SCC 143, AIR 2007 SC 493
[25] Section 1(2) of IT Act, 2000.

computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorised user or tampers etc…he shall be liable to pay damages to the person so affected. Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008[26].

II. Section 66 C- Punishment for identity theft. -Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

III. Section 66 D- Punishment for cheating by personation by using computer resource. -Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

IV. Section 66 E- Punishment for violation of privacy. -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 with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation. -For the purposes of this section-

i. "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

ii. "capture", with respect to an image, means to videotape, photograph, film or record by any means;

iii. "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

iv. "publishes" means reproduction in the printed or electronic form and making it available for public, and;

v. "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that; -

(a) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

[26] *Supra* Note 4.

(b) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place. Section 67- Publishing or transmitting obscene material in electronic form[27]

Cyber defamation, cyber defamation, email spoofing, cybersex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 506 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women. [28] Recent amendment in IPC have added sections 354 C and 354 D which deal with voyeurism and stalking respectively.

Voyeurism[29]:

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 on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.

Explanations-

i. For the purpose of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

[27] Karnika Seth, Computers Internet and New Technology Laws (*Lexis Nexis*, 2013)
[28] *Supra* Note 14
[29] Criminal Law (Amendment) Act, 2013

ii. Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.

FINDINGS

Cybercrimes have become a root cause of a crime as these days it is very easy to gather information about a lady just with a click on the computer. Not only it is being used at an early stage to understand a human behaviour but even to defame a person it is used as a media. Her identity in a place she values-cyberspace, and the communities of which she is a part in that world-shifts from whatever she was-student, lawyer, software engineer, technician, teacher, wife, lover, blogger, friend -to what she is repeatedly called: cunt, slut, whore, bitch, liar, fraud, incompetent, stupid. The economic and professional or vocation harms are equally profound. She may lose clients and customers and ultimately curtail her career, if her business has been ruined by the online defamation and harassment. She can't find a job**,** or seek a promotion, if she can't risk her current or potential employers doing a Google search. She lives in fear of discovery. And lastly, her civic participation-including her freedom of speech-is drastically curtained.

In the case, *Dr. L. Prakash v. Superintendent*[30], the accused was an Orthopedic Surgeon forced women to perform sexual acts and later on upload and sale these videos as adult entertainment materials worldwide. He was charged under section 506 (part II of the section which prescribes punishment for criminal intimidation to cause death or grievous hurt), 367 (which deals with kidnapping or abduction for causing death or grievous hurt) and 120-B (criminal conspiracy) of the IPC and Section 67 of Information Technology Act, 2000 (which dealt with obscene publication in the internet). He was sentenced for life imprisonment and a pecuniary fine of Rupees 1, 25,000 under the Immoral Trafficking (Prevention) Act, 1956.

Yet in the case of *State of Tamil Nadu v. Suhas Katti*[31], the accused Katti posted obscene, defamatory messages about a divorced woman in the yahoo message group and advertised her

[30] (2008) 3 MLJ (Crl) 578
[31] naavi.org Chennai Cyber Crime Cell gets its first case in record time available at www.naavi.org/cl_editorial_04/suhas_katti_case.htm (last accessed on October 07, 2017).

as a solicit for sex. This case is considered as one of the first cases to be booked under the Information Technology Act, 2000 (IT Act). He was convicted under section 469, 509 of Indian Penal Code (IPC) and 67 of the IT Act 2000 and was punished for 2 years rigorous imprisonment and fine. Above mentioned cases were considered first time under the ambit of IT Act. Apart from these cases there are few basic cybercrimes that basically happens to the Indian women in the cyberspace such as harassment via e-mail, cyber-stalking, cyber defamation, morphing, email spoofing, hacking, cyber pornography and cyber sexual defamation, cyber flirting and cyber bullying.

In a survey, it was evident that the conviction rate of cases with respect to cybercrimes in various states is poor. It is important to note that Andhra Pradesh ranks high in cybercrimes against women. Telangana, a state formed just two years ago, has recorded 16 cybercrime convictions till date (three times more than Maharashtra) whereas U.P. has been recorded 89 conviction rates. Also, it has been observed that Maharashtra has the maximum number of cases registered. The state has saw a steep 142.1% rise in registration of cybercrime cases from 907 in 2013 to 2,195 in 2015. Experts say the 'normal judicial process' is unable to handle the unique nature of cybercrimes. Also, the cyber criminals use proxy servers that investigating agencies find difficult to trace.[32]

Yet there are many cases which are happening in the day to day life. Even travelling isn't safe anymore. It can be well witnessed with the increase cyber crime rate in the cab service as well. The cab is booked online so as to travel but the driver himself takes the advantage of a woman travelling alone. A case of voyeurism was registered by the Delhi police against an Ola driver on complaint of the passenger woman for focusing camera towards her while she was busy on her mobile phone.[33]

CONCLUSION

Tackling online abuses is a global problem. The Internet is an unparalleled global communications medium. However, online interactions can be harmful, leading to emotional suffering and physical harm. The current legal system has gone some way towards protecting

[32] V. Narayan "Cyber Crime Convictions in Maha: Just 5 out of 4,980 cases in 3 years" *The Times of India*,July, 29, 2016
[33] Staff Reporter "Ola Driver Arrested", *The Hindu* (July 21, 2016)

victims of online harms. However, the law still has a long way to go. Legal remedies will always suffer limitations related to time, cost, and jurisdictional challenges in a borderless online world. Like many other aspects of internet regulation, effective responses to online abuse will require a multi-modal regulatory framework. Regulatory modalities such as social norms, public education and market forces will need to interact to create more comprehensive responses to online abuses. In an initiation by the INTERPOL which coordinated joint efforts among police in five countries (including Russia, Netherlands and USA) to take down Simda Botnet, which was thought to have infected over 77,000 computers[34], such initiations are required to be undertaken by the government so as to curb this menace.

The Information Technology Act, 2000 is a great step forward and it is the right initiative at the right time. There is no doubt that such a law is absolutely necessary in the country today. But the only problem which is being faced by IT Act, 2000 now is that cybercrime is emerging and evolving concept, everyday new forms of criminal activities in cyberspace are coming to the forefront. Due to this reason IT Act is not fully capable to deal with every aspect of cybercrimes. Hence, a need is felt for more stringent laws.

SUGGESTION

The police must be given training with respect to gathering of evidences in such cases because most errors are committed by investigating staff while seizing computer systems. Current approaches to online abuse might be improved if the existing commercial services could be supplemented with more easily affordable pro bono services, and if individuals could be empowered themselves to engage proactively in reputation management strategies.

Greater awareness among the general public is needed. They are required to take necessary care while using the cyberspace. In other words, people must be told about not disclosing their personal details on it. Moreover, the rights of a victim and redressal mechanism should also be explained. Hence, it is the need of the hour that the subject dealing with various cybercrimes be made a compulsory subject at primary level. One must not blindly out of habit of download free apps and accept sensitive terms and conditions resulting in data leakage, Ids and other information. There is a need of public prosecutors who are well versed with the IT Act so that

[34] Sanjay Gade, *How Cybercrime is Evolving, Lawyers Update* (May 2016)

justice is delivered. Not only public prosecutors but Judges are also required to understand the various provisions for this purpose.

In order to give effect to hypothesis, it is essential to have a universal legal framework which should accepted globally, backed by specialized and fully equipped law enforcement mechanisms and appropriate awareness among masses would go a long way in controlling and abetting these cybercrimes. This is only possible when countries reach a consensus as to which computer and technology related activities should be criminalized and then accordingly domestic laws should be altered.