LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

INTERNET- WELFARE OR A WEAPON? [1]

INTRODUCTION

"More and more, modern warfare will be about people sitting in bunkers in front of computer screens, whether remotely piloted aircraft or cyber weapons."

-Philip Hammond

The above quote elucidates that, in the modern era of digitization, war no longer leads to bloodshed or conquering borders rather, it is intruding into a person's personal life and privacy via internet. Off late, we witness and hear news that the government has identified drones flying in restricted airspaces controlled from across the border to understand our strategic positions as against the conventional methods of sending soldiers who cross a border and sneak into our land. The most important element in any war or counter attack is communication. There has been an increase in cyber warfare through which the hackers hack into the main communication servers to break communication among the soldiers and even try to extract highly classified information from government databases.

Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies.[2] The term cyber-crime needs no introduction in today's e-world, where crimes are being committed at a click of mouse. Cyber-crime thus, is the darker side of technology. It is no different from a traditional

[1] Mr.Manik Taneja, 3rd Year (5th Sem),Vivekananda Institute of Professional Studies, GGSIPU, New Delhi & Ms. Muskaan Chadha, 3rd Year (5th Sem),Vivekananda Institute of Professional Studies, GGSIPU, New Delhi.

[2]Talwant Singh, "Cyber Law & Information Technology", India, *available at*: http://www.delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf (last visited on March 31, 2017).

crime. The only difference is that it involves technology. Technology was made to improve the human life but now it is exploited by criminals. Defining cybercrime as an act, that is punishable under the Information Technology Act, 2000 would be unsuitable as the Indian Penal Code also, covers many cyber-crimes, such as email spoofing and cyber defamation, sending threatening emails, etc. A simple yet a sturdy definition of cyber-crime would be "unlawful acts wherein the computer is a tool or a target or both."[3]Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime. It is rapidly evolving from simple e-mail mischief where offenders send obscene e-mail, to more serious offences like theft of information, e-mail bombing to crashing servers etc. Yet cyber-crimes have increased over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities.

This article highlights the issue of cyber-crime. An attempt has been made to discuss the issues and challenges related to it. Also, it talks about its relevance in India as well as how is it different from the rest of the world. This article also highlights the developments related to women safety in the cyber space.

(I) ISSUES AND CHALLENGES

[3]Cyber Law in India: Introduction, India, *available at:* www.cyberlawsindia.net (last visited on March 31, 2017).

The world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind, but in today's scenario it is being used for the criminal acts. Each society have been providing its own description of criminal behavior and conduct made punishable by express will of the political community ruling over the society and it was always influenced by religious-social-political economical values prevailing in the given society[4].Cyber-crime is the latest and perhaps the most complicated problem in the society. It can be committed against the person, against person's property, against the government and the society at large.

Cyber-attacks are global, cyber security risks are universal[5]. Almost all systems, are prone to cyber-attacks all over the world. Today's scenario is that hackers are proactive whereas the concerned authorities responsible for ensuring security and reliability are reactive. The foremost concern is that our data is stored somewhere else owing to the availability of cloud storage accounts that are proving free cloud space.

Unequivocal issues demanding more attention of the authorities are:

- Emphasis on the product development where security and privacy are assured in software designs.
- Create mechanisms which will provide avenues for reformed methods for cyber-attack detention.

[4]Sumanjit Das,TapaswiniNayak, "Impact of Cyber Crime: Issues and Challenges", India, *available at:*http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf, (last visited on March 31, 2017).

[5] NJ Rao, ''Cyber Security: Issues and Challenges'',India, *available at:* http://www.csi-india.org/communications(last visited on March 31, 2017).

- Concoct manpower with better qualification and training to deal with the issue of cyber-security.
- Better formulation of risk mitigation strategies.
- Mechanisms for safeguarding digital rights and protecting privacy.
- Establish protocols for creating increased awareness on the issue of cyber-crime.

The threat from cyber-crime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cyber-criminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of organized crime and terrorism[6].

Various challenges are associated with cyber-security when it comes to cyber-crime, some of these challenges are:

- The unprecedented rise in the industrialization of a type of crime where the commodity, personal information, moves far too quickly for conventional law enforcement methods to keep pace with and threatens the ability of the authorities to respond with millions of virus and other types of malicious code.
- Mobile internet access and the continuing deployment of broadband internet infrastructure throughout the world therefore, introducing new levels of vulnerability.
- One of the most alarming problems is the easy availability of child pornography.

Another challenge for national authorities is to overcome jurisdictional restrictions by coordinating regionally or with agencies with similar level of capacity to understand better and respond to internet-facilitated crime.

There seems to be a quantum jump in unethical practices and corruption. Measures should be taken to vanquish the issues and challenges pertaining to cyber-crime such as advancements in technological solutions and ease on their availability without compromising on privacy and

[6]Rajarshi Rai Choudhury, "Cyber-crime-Challenges and solutions", 4 *IJCSIT* 5 (2013).

security, ensuring creation of suitable human resources which is ahead of time and at the same time be well capped with social necessity ensuring freedom.

The need of the day is to facilitate such cyber systems which would meet the basic parameters of utility, cost and ease along with the security and privacy.

(II) CYBER CRIMES IN INDIA-

"When a man is denied the right to live the life he believes in, he has no choice but to become an outlaw."

-Nelson Mandela

India has emerged as one of the primary targets among cyber criminals with growing adoption of internet and smartphones. Myriad of challenges being tackled in the India being most populated country.The conspicuous one is the fact that still internet access is quite confined to some places however the users are very naïve that they could be hacked so easily. This is also a threat to the vision of Digital India which can be only achieved when there is less cyber security risk. There was an increase of 300%in relation to cyber-crime between the years 2011-2015.[7]There was a shoot up of cyber-crime after demonetization.[8]The rise of the cyber-crime is a big issue. many steps are being taken by the Government of India. The remedies available for the cyber-crimes in India are given under andare registered under the head of Information Technology Act2000; offences are defined under chapter 11 of the Act. The other heads under which the cybercrime case can be registered are Indian Penal Code and Special and Local Laws. There are around 50 offences which are covered under cyber laws in India such as tampering with computer source documents given

[7] Rakesh Dubbudu, ''most number of Cyber Crimes reported in Maharashtra & Uttar Pradesh", *available at:*https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/ (last visited on March 31, 2017).

[8]SiddharthTadepalli, Cyber crime cases shoot up post demonetization, *Times of India,* December 23, 2016, *available at:* http://timesofindia.indiatimes.com/city/hyderabad/Cyber-crime-cases-shoot-up-post-demonetisation/articleshow/56129277.cms?TOI_browsernotification=true (last visited on March 31, 2017).

under Section 65 of the IT Act, 2000, e-mail abuse given under Section 500 of the Indian Penal Code, 1860 etc.[9]

(III) LEGISLATIVE DEVELOPMENTS-

In the knowledge society of 21st century, computer, internet and ICT or e-revolution has changed the life style of the people. Accordingly there was enhancement in the use of technology and the development towards electronic platform. Apart from the positive side of e-revolution, there was also an increase in the number for crimes with the usage of computer as a tool or a target for committing a crime[10]. A new branch of jurisprudence was required to tackle the problems related to the cybercrime, also to regulate e-commerce. India was signatory member of the United Nations Commission on International Trade and Law (UNCITRAL Model) in the year 1996 and it was also adopted by General assembly by passing a resolution in the year 1997.[11]Later, India had to amend national laws according to the Model Laws for the regulation of e-commerce and to provide security to the E-transactions, which resulted in the enactment of The Information Technology Act, 2000 (hereinafter the IT Act, 2000). The said act is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format.[12] With the passage of time, there were some new challenges which were not covered under the said Act. For removing the deficiencies, Government of India passed Information Technology Amendment Act, 2008 (hereinafter the ITA Act, 2008. Also, after

[9]Cyber Laws in India, *available at:* http://www.cyberpolicebangalore.nic.in/pdf/Cyber%20law%20IPC.pdf (last visited on: March 31, 2017).
[10]Computer Crime, United Kingdom, *available at:*http://www.parliament.uk/documents/post/postpn271.pdf (last visited on March 31, 2017).
[11]Information Technology Act, 2000, India, *available at:* https://en.wikipedia.org/wiki/Information_Technology_Act,_2000 (last modified on March 8, 2017).
[12] Salient feature of IT Act – A comparative study, *available at:*https://www.legalbites.in/salient-feature-of-it-act-/ (last visited on March 31, 2017).

'the December 2012 Delhi gang rape incidence'[13], the Indian government has taken several initiatives to review the existing criminal laws and amendments were done in the year 2013.The Criminal Law (Amendment) Act, 2013 added Section 354D in the Indian Penal Code, 1860 to define and punish the act of stalking.

(IV) JUDICIAL DEVELOMENTS-

Cyber law incorporates cyber-crimes, electronic commerce, freedomof expression, intellectual property rights, jurisdiction issues and choice of law, and privacy rights.The definition of what constitutes a crime in cyber space is still being developed. In the past, the states and federal government defined cyber-crime activities to include the destruction or theft of computer data and programs. More recently the definition has expanded to include activities such as forgery, illegal gambling, cyber stalking, cyber defamation etc.There are several areas on the internet where there is a real risk of liability for defamation.

In 2001, India's first cyberstalking case was reported. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. RituKohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of RituKohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding

[13]ShubhomoySikdar, Delhi gang-rape: victim narrates the tale of horror, *The Hindu*, December 23, 2012, *available at:* http://www.thehindu.com/news/national/delhi-gangrape-victim-narrates-the-tale-of-horror/article4230038.ece (last visited on March 31, 2017).

protection of victims under the same. While there is no record for subsequent proceeding, this case made Indian legislator's wake up to the need for a legislation to address cyber stalking[14].

In *Shreya Singhal v. Union of India*[15], the Supreme Court struck down Section 66A of the Information Technology Act, 2000, relating to restrictions on online speech, unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1) (a) of the Constitution of India. The Court further held that the Section was not saved by virtue of being 'reasonable restrictions' on the freedom of speech under Article 19(2).

Section 66A of Information Technology Act includes 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 by making use of such computer resource or a communication device; or

(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.

Defamation laws vary from country to country and in countries such as the Canada, Australia and the United States, it can vary from province to province and state to state. Therefore, plaintiffs may have the luxury of "forum shopping" or choosing the jurisdiction with the laws most favorable to him/her[11].

[14]P. Shah, Cyber Stalking & the impacts of legislative provisions in India, *available at:* http://www.legalindia.in/cyber-stalking-the-impact-of-its-legislative-provisions-in-india (last visited on March 31, 2017).

[15]Writ Petition (Criminal) No.167 Of 2012.

In *Stratton Oakmount v. Prodigy* (1995), the US Supreme Court provided no incentive for online service providers to remove obscene or libelous material from their databases. If any good faith attempt were made to inspect content prior to publication, the online service provider risked liability for any offensive material it missed. This case led to the enactment of the Telecommunications Act of 1996, and was effectively overruled by the said Act.

*New York Times Company v. Sullivan*was a U.S. Supreme Court case which established the actual malice standard before press reports could be considered to be defamation and libel; and hence allowed free reporting of the civil rights campaigns in the southern United States. It is one of the key decisions supporting the freedom of the press. The actual malice standard requires that the publisher knows the statement is false or acts in reckless disregard of the truth.

The decision established that for a plaintiff to win a libel ruling against a newspaper, "actual malice" or "reckless negligence" must be proved on the part of the paper if the statement in question is about a public official or public figure. In the case of a private figure, the plaintiff must merely prove negligence.

(VI) Position in India-

The Information Technology Act 2000 was passed by the Parliament of India in May 2000, aiming to curb cyber-crimes and provide a legal framework for e-commerce transactions.

The Delhi High Court has passed an ex-parte ad interim injunction in the case entitled "*SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra"*[16], India's first case on cyber defamation. In this case, the defendant Jogesh Kwatra being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The plaintiffs filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiffs. The Delhi High Court

[16]CS(OS) No. 1279/2001.

passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiffs. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments.

The case of *Tamil Nadu v SuhasKatti*[17] is worth mentioning for the fact that the conviction was successfully achieved within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time. The case is related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. "The accused was found guilty for offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused was convicted and sentenced for the offences to undergo rigorous imprisonment for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000." To secure Justice, Judiciary plays a vital role in shaping the enactment[18] according to the order of the day.

(VII) CONCLUSION-

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided. The truth is that the criminals have changed their methods and have started relying on the advanced technology.There are 13 root servers across the world. 10 root servers are in USA, 1 in Sweden, 1 in Japan and 1 root server in the Netherlands. India on date, does not have a root server which is essential to keep the important and official data. Also, at present the current

[17]*Tamil Nadu v SuhasKatti* (2004)

[18]Mohak Rana, Crimes in Cyberspace: Right to Privacy and Other Issues, *available at:* https://www.lawctopus.com/academike/cyber-crimes-other-liabilities/ (last visited on March 31, 2017).

internet connectivity protocol is IPv4 and IPv6 is a replacement to it. It is being developed as a critical technology meant to address the growing concern of safety, sustainability as well as the ease of administration. IPv6 would not only ensure safety but would also provide various effective measures to curb the issue of cyber-crime. Switching to IPv6 as well as introducing a root server would be of utmost importance in order to ensure safety against cyber-crimes.

Cyber-crime is a global phenomenon. With the advent of technology, cyber-crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Even though India is one of the very few countries to enact IT Act 2000 to combat cyber-crimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the security of women in general is not covered fully by this Act[19].

The Government has taken following steps for prevention of Cyber Crimes:-

i) Cyber Crime Cells have been set up in States and Union Territories for reporting and investigating Cyber Crime cases.

ii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

iii) In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training

iv) Workshops on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber-crimes for judicial officers.

[19]Debarati Halder, Cybercrime against Women in India, *available at*: http://www.cyberlawtimes.com/articles/103.html (last visited on March 31, 2017).

v) Training is imparted to Police Officers and Judicial officers in the Training Labs established by the Government.

vi) The Scheme for Universalization of Women Helpline has been approved to provide 24 hour emergency and non-emergency response to all women affected by violence.

Though actions have been taken to combat the issue of cyber-crime but there is still a long way to go. Every effort should be made to harmonize the laws on cyber-crime in such a way as to facilitate international cooperation in preventing and combating these illicit activities as well as consider various measures, including setting up a Voluntary Specific Fund, to support efforts to expand cooperation on this matter in the Hemisphere.