RESEARCH PAPER | Law | Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

Cyber Crimes and New Challenges Before Mordern Society

KEYWORDS

Adv.Syed Rahmat Quadri

LL.M DCL, Quadri House, Mali Base, Parbhani(MS)-431401

Introduction:-

The stakes involved in cyber crimes are more serious due to the inherent characteristics of the network functioning. With the help of technology, the criminals are able to conduct their activities in much more sophisticated manner and within the relative safety of their homes or other private places, continents away from the actual 'scene of crime'. Other characteristics of computer network that increase their vulnerability to crimes include;

- Density of information and processes in the network
- Relatively easy accessibility to the system
- Vulnerability due to dependence on telecommunication systems
- Uncertainties of the complex logical processes

Traditional responses to crime become irrelevant in fighting this technological menace. We need innovative strategies and technologies to catch up with the criminals and keep abreast of them, who are coming out with newer and newer versions of cybercrimes. Otherwise, the potential of this great revolution of Internet and computer will never reach their maximum. Cyber crimes are very serious threat for the time to come and pose one of the most difficult challenges before law enforcement machinery. To combat crime in cyber space we have to implement strict and advance statutes which cover the area of cyber crime.

As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails, to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyber law issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyber law for your own benefit.

Internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of, be it entertainment, business, sports or education. Internet has also its own disadvantages one of the major disadvantage is cyber crime. The internet along with its disadvantages has also exposed citizens to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like email espionage, credit card fraud, spasm, software piracy and so on criminal activities in the cyberspace are on the rise.

Concept of Cyber Crime:-

In the growing world of internet, both in personal & in internet business, There is an ever increasing problem with cyber crime. Punishment for these crimes has become a new field in crime investigation & law enforcement. Cyber crime has taken criminals across borders & limitations that nothing else has been able to do, until the advent of the internet. Where a door is left open, the criminal element will final their way in. In this case, the door for crime is the internet. Cyber crime is vast in scope. It ranges from the individual criminal to an increasing presence of International Organized Cyber Crime. Scams run rampant across the internet. They fill email boxes & websites, trying to lure unsuspecting victims into their webs of deception.

Crimes of more personal natures also abound across the internet. Dating & chat sites are rife with scammers or people playing dangerous games with individual human victims. The social interaction becomes a crime, when the person becomes victimized by cyber stalkers or people who use the internet to bolster some insecure or ill ego, at the expense of a real human being. Children are often victims of these crimes too.

Maintaining security & safety on the Internet has become increasingly more complex. Whole companies & businesses exist to deal with the problems. Law enforcement agencies worldwide now have special units which work on nothing but cyber crimes of all kinds. Cyber Crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.

The computer may be used as a tool in the following kinds of activity:-

Financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, Cyber defamation, cyber stalking. The unlawful acts in the following cases: - Unauthorized access to computer, theft of information contained in electronic form, email bombing, data dialing, Trojan attacks, web jacking, theft of computer system, physically damaging the computer system. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government.

In short, cyber crimes taking place in the society can be enumerated as follows;

1. Financial Crimes involving cheating, credit card frauds, money laundering, Etc.
2. Cyber Pornography involving production and distribution of pornographic material.
3. Sale of illegal articles such as narcotics, weapons, wild

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

life etc.
4. Online Gambling
5. Intellectual Property Crimes such as theft of computer source code,
6. Software piracy, copyright infringement, trademark violations, etc.
7. Harassments such as Cyber Stalking, cyber defamation, indecent or abusing mails, etc.
8. Forgery of documents including currency and any other documents
9. Deployment of viruses, Trojans and Worms Cyber Attacks and Cyber Terrorism

Legislative & Judicial Perspective:-

1. Information Technology Act, 2000:-

In India, the information Technology Act, 2000 was enacted after the United Nations General Assembly Resolution dated 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by United Nations Commission on International Trade law.

The Indian Parliament considered it necessary to give effect to the resolution.

As a consequence of which the information Technology Act, 2000 was passed & enforced on 17th May, 2000. India became the 12th nation in the world to adopt a cyber law regime; it covers areas like e-governance, e-commerce, cyber contraventions & cyber offences. The cyber laws of India are contained in the information Technology Act, 2000.

The Act aims at providing legal recognition for transactions carried out by means for electronic data interchange & other means of electronic communications commonly referred to as "electronic commerce" which involves the use of alternative to paper based methods of communication of storage of information & aims at facilitating electronic filing of documents with the government agencies.

Key Highlights of the Act -

Highlights of the Act are listed below…

Chapter II of the IT Act Specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

Chapter III of the IT Act details about Electronic Governance & provides interlaid amongst others that where any law provides that information or any other matter shall be in writing or in typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information is rendered or made available in electronic form, & is kept accessible to be used as subsequent reference.

Chapter - IV of the Act gives a scheme for regulation of Certifying Authorities. The Act envisages a controller of Certifying Authorities who shall perform the function of exercising supervision over the actives of the certifying Authorities as also laying down standard & conditions governing the certifying Authorities. The Act recognizes the need for recognizing the need for recognizing foreign Certifying Authorities & it further details the various provisions for the issue of license to issue Digital Signature Certificates

Chapter VII of the Act details about the scheme of things relating to Digital Signature Certificates & duties of the Subscribers enshrined in the Act.

Chapter IX of the Act talks about penalties & adjudication for various offences.

Chapter X of the Act talks about the establishment of Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the adjudicating officers shall be preferred.

Chapter XI of the Act talks about various offences which shall be investigated only by a police officer not below the rank of Deputy Superintendent of police.

2. Indian Penal Code, 1860:-

Information Technology Act of 2000 is versatile enough to accommodate those aspects of cyber law which should have been covered by IT Act 2000 but are covered by other statutes. Thus since any IPC offence committed with the use of "Electronic Documents" can be considered as crime within the definition of a "Written Documents", "Cheating" "Conspiracy", "Breach of trust" etc. This, in addition to Information Technology Act, 2000 provisions of Indian penal code is also applicable to cyber offences.

The Indian Penal code extends to the whole of India except the state of Jammu & Kashmir. It contains 23 chapters with 511 Sections.

IPC applies to every person including a foreigner for any violation committed in India. Under some circumstance, IPC also applies to offences committed abroad.

IPC as amended by the IT Act Contains several provisions that penalize cyber crimes.

These include -

- Sending threatening message by email
- Sending defamatory messages by email
- Forgery of Electronic records
- Web Jacking
- Obscenity & Pornography

Indian Evidence Act, 1872:-

The nature of electronic evidence is such that in almost all cases where any electronic record is to be produced as evidence, it will actually be a copy of the original record that will be exhibited & not the original. Keeping in mind the peculiarities of digital evidence, Indian Evidence Act was amended by the IT Act, 2000.

The most important amendment was the admissibility of electronic records as evidence in court of law. The computer holding the original evidence does not need to be produced in court. A printout of record or a copy on a CD ROM, hard disk, floppy etc. can be produced in court. However, some conditions need to be met & a certificate needs to be provided

Conclusion:-

A major problem in writing, enforcing, prosecuting & interpreting cyber crime laws, is the lack of technical knowledge on the part of legislators & experts charged with these duties. Legislators, in most cases, do not have a real understanding of the technical issues & what is or not desirable – or even possible to legislate. Police investigators are becoming more technically savvy, but in many small jurisdictions, no one in the department knows how to re-

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

cover critical digital evidence. Judges often have a lack of technical expertise that makes it difficult for them to do what court do: interpret the laws. The fact that many computer crime laws use vague language exacerbates the problem. The answer to all these dilemmas is "Education & Awareness Programmer". These programs must be aimed at everyone involved in the fight against cybercrime, including –

1. Legislators & other Politicians
2. Criminal Justice Professionals
3. IT Professionals
4. The community at large & the cyberspace community in particular

REFERENCE 1) www.legalserviceindia.com/article/146 | 2) Cyber law in India' (Law on Internet) by Dr.Farooq Ahmed | 3) Systematic approach to information technology 'by Sujata Garg, 1stEdi, 2005, pub by D.C. Puliani for Bharat Law House Pvt. Ltd. New Delhi. | 4) Cyber Law "by Justice Yatindra Singh, 3rd Edi, 2007, pub. By Universal Law Publishing Co. Pvt. Ltd, Delhi, | | 5) Cyber crime' by B.R.Puri and T.N.Chhabra,1st ed,2002, pub, by Pentagon Press , Delhi Fundamentals Of Cyber Law By Rohas Nagpal | 6) Information technology act 2000 | 7) The simple economics of cyber crime" by Nir Kshetri | 8) Law of cyber Crimes & Information Technology Law" by S. V. Joga Rao, 1st ed. 2007, Pub. by Wadhawa & Company, Nagpur. |