ISSN 2454-8596
www.MyVedant.com

An International Multidisciplinary Research E-Journal

Cyber Crime And Its Control By Enacting Law's In India : A Legal Analysis

Dr. Dhanani Sanjaykumar G.

LL.M., Ph.D.

IN. PRINCIPAL

Shree H. M. Patel Mahila Law College

Joshipura , Junagadh

Gujarat

ISSN 2454-8596
www.MyVedant.com

An International Multidisciplinary Research E-Journal

ABSTRACT:-

Information technology an important and indispensable to the life of human beings. Transmission, recording or memory and processing of information are three essential processes of information. Computers are a major segment of the new information technologies. With the help of satellite communication, the transmission of data has become very fast. The data can be telexed, the voice over a telephone can be transmitted on local, national and international network. The computer is a boon or a bane depends on its use. If used for the benefits of the mankind it is a boon, if used for the evil purpose it is a bane. This study aims to the technological transformation of crime the streets to the networked super highways of cyberspace. Cyber crime to day has the potential to affect the lives of each and every one of us. The laws relating to cyber crime are quite complex. Under the frame work, simple things we unwittingly do online may be punishable and severe offenses may go unnoticed. Hence the need to know more about the how cyber crime is policed in the Indian context and what laws govern Indian cybercrime.

Keywords : Cyber Crime, Cyber Security Incident, Illegal down loading, Cyber Hacking, Cyber Security Breaches, Cyber Crime Acts.

INTRODUCTION :

Charles Babbage developed the first analytical engine in 1812. This machine had the concepts of modern computers namely memory, arithmetic unit and capacity to handle stored programme. But this machine could not be put into practical applications due to technological limitations at that time. In 1854, George Boole, invented the logic system which is the basis for today's digital computers. In 1937, the first electro machine calculator was developed by Howard and Aitten. In 1946, the first computer came into existence. It was named as ENIAC (Electronic Numerical Integrator and Calculator). It was developed by Dr John Nouchly and J.P. Eckert of the University of Pennsylvania, USA. In 1951, Remington Rand corporation of USA brought out a commercial computer named UNIVAC (Universal Automatic Computer). These computers had the short coming of value technology. They were slow in operations and un reliable. These computers were named the first generation equipment. Transistor technology gave advent of second generation of computers. These were smaller in size, but more reliable and had higher speed of operation. Third generation computer consisted of IBN-370 type. The fourth generation computer, presently manufactured by USA, Japan and other European and Asian Countries are based on large scale integration. Better Computers are under trail in USA and Japan. These are based on artificial intelligence. They will think like the human brain, collect most information from their reservoir of memory, make expert judgement and decisions.

REVIEW OF LITERATURE :

The word computer comes from the word 'Compute' that means to calculate. So a computer was normally considered to be a calculating device that can perform arithmetic calculations at an enormous speed and with perfect accuracy. But now-a-days more than 80% of the work done by computers is of non-mathematical or non numerical nature. Today the computer has become cornerstone of our

industrial and scientific development. The computers have shrank the world into a room. In all walks of life from manufacturing of a small item, to exploration of ocean and space, computers are being used extensively. The computers on the one side helped the mankind to solve many crucial problems, on the other side it has put the world at the verge of destruction. In spite of that it is not at all the fault of the computers it self. It is a machine which obeys the orders of the user, therefore, fault lies with the user not with the computers.

Upto 1990's the Internet was largely used by Academic, Government and Industrial researchers. But with the invention of new application the www (world wide web) millions of new non academic users were added to the Internet. Internet is a web which has a very large numbers of computers connected to each other. These computers are connected with one and another either through wire, satellite, microwaves. Internet is essentially a big network that links smaller net works and individual computers all over the world using modems, phone lines and satellite links. With the easy availability of Internet access, the internet is being misused not only by the youth and but also by the matured people. The government has to tackle this situation in order to keep the youth away from such sites enacted the Act called the Information Technology Bill having been passed by both the Houses of Parliament, received the assent of the President on 9th June, 2000. It came on the statute book as the Information Technology Act 2000. The Information Technology Act 2000 came into force on 17th October 2000. As per the Information Technology Act 4 [(nb) cyber 'security' means protecting information, equipment, devices computer, resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction;]. 4 [(ze) 'Secure System' means computer hardware, software and procedure that :

are reasonably secure from unauthorized access and misuse;

Provide a reasonable level of reliability and correct operation.

Are reasonably suited to performing the intended functions.

Adhere to generally accepted security procedures.

OBJECTIVE OF THE STUDY :

To discuss what is cyber crime ?

To discuss various types of cyber crime.

To discuss the existing Indian laws pertaining to cyber crime and how various crimes are treated.

To discuss punishment for computer related offences as per the existing IT Act 2000 and IT amended Act 2008.

To discuss the cyber security by Government of India.

To suggest some safety tips to users for check cyber crimes.

STUDY METHODOLOGY :

Sources of Data -

Books, Journals and Magazines.

News Papers

Law Magazines and Law Books

Internet

SCOPE OF STUDY :

The scope of study is limited to theoretical and conceptual analysis. The accuracy of the study is limited to the accuracy of these sources.

FINDINGS AND DISCUSSIONS :

What is Cyber Crime ?

Cyber Crime means any illegal activity committed using a computer and / or the internet can be called a cyber crime. Cyber crime is basically an extension of existing criminal activity. Studies show that on an average more than one cyber crime occurs every 10 seconds. There have been recorded losses of over $500 million in one year solely due to cyber crime. The crime is basically an attack on information about people or groups, and though the attack is not physical (it's virtual), it is equally harmful. The most common targets of cyber criminal activity are found to be government offices and financial institutions. The majority of teenage hackers are doing it for the motive of recreation rather than for profit or causing harm.

Why Cyber Laws Enacted ?

As a result of the technological advancement in the IT industry, computers and internet became accessible to the common man in our country quite rapidly. Like any technology, IT too met with two kinds of people – the users and the abusers. While cases of hacking cam to light and identity, privacy and information security was found to be increasingly compromised by the new IT revolution, the need was felt for law and order mechanism in the electronic world too.

Cyber Laws :

Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. This law same as any other branch of law, help what is legal and illegal and stipulate mechanism to detect, convict and punish offenders and protect electronic property and its rightful use. Cyber laws pertain to diverse aspects of the electronic world such as :

Software licences, copyright and fair use.

Unauthorized access, data privacy and spamming.

Export of hardware and software.

Censorship.

Computerized voting.

IT ACT 2000 AND IT (AMENDMENT ACT, 2008) :

The Information Technology (IT) Act 2000 was passed by the Indian Parliament in May 2000 and came into force on 17.10.2006 of the same year. Its Prime Purpose is to provide the legal infrastructure for e-commerce in India. It was the first legal instrument to provide legal sanctity to electronic records and contracts expressed through electronic means of communication. The act was later amended in December 2008 through the IT amended Act, 2008 and came into force 27.10.2009. The two IT Acts together define below.

Digital Signatures : Electronic records may be authenticated by a subscriber by affixing digital signature; further, the signature may be verified using the public key provided by the subscriber.

Certifying Authorities : Domestic and foreign certifying authorities (which provide digital signature certificates) are recognized by the law : a "controller of certifying authorities" shall supervise them.

Electronic Governance : Documents required as per Law by any arm of the government may be supplied in electronic form, and such documents are to be treated the same as hand written, type written or printed documents.

Offences and Penalties : An adjudicating officer shall judge whether a person has committed an offence in contravention of any provision of the IT Act, 2006; the maximum penalty for any damage to computers or computer systems is a fine upto Rs.1 crore.

Appellate Tribunals : A cyber Regulation Appellate Tribunal shall be formed which shall hear appeals against orders passed by the Adjudicating Officers.

Investigation : Offences shall only be investigated by a police officer of the rank of the Deputy Superintendent of Police or above (amended to the rank "Inspector" or above by the IT amendment act 2008).

Amendment to other Laws: Other Acts such as the Indian Penal code 1860, the Indian Evidence Act 1872, the Bankers Book Evidence Act 1891, the Reserve Bank of India Act 1934 were to be amended to align them with the IT Act.

Network Service Providers : Intermediaries in the data transmission process, such as Internet service providers, are not liable in certain cases, so long as the intermediary

expeditiously acts to prevent the cyber crime on getting such instruction from the Government or its agency.

PUNISHMENT FOR COMPUTER RELATED OFFENCES AS PER IT ACT 2000 AND IT (AMENDED ACT) 2008 :

Under Section 65 :- Tampering with computer source documents such as alter any computer source code, computer programme, computer system, computer network, shall be punishable with imprisonment upto three years or with fine which may extend up to two lakh rupees or with both.

Under Section 66 :- Where a body corporate possessing or handling any sensitive data or information in a computer resource dishonestly or fraudulently, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Under Section 66 (A) : Any information that is grossly offensive, false, danger, ill will, criminal intimidation use any electronic mail message shall be punishable with imprisonment for a term which may extend to three years and with fine up to two lakh rupees or with both.

Under Section 66 (B) : Punishment for dishonestly stolen computer resources or communication device shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Under Section 66 (C) : Punishment for identify theft such as electronic signature, password any other identification feature of any other person shall be punished

imprisonment of three years and shall also be liable to fine with may extend to rupees one lakh.

Under Section 66 (D) : Punishment for cheating by personating by using computer resource shall be punished with imprisonment for a term which may extend to three years and shall also be liable to fine which may be extend to rupees one lakh.

Under Section 66 (E) : Punishment for violation of privacy whoever, intentionally or knowingly captures, publishes the image of a private area of any person without his or her unsent shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Under Section 66 (F) : Punishment for cyber terrorism : (i) who ever with intent to threaten the unity, integrity, security or sovereignty of India to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Under Section 67 : Punishment for publishing or transmitting obscene material in electronic form shall be punished for a term which may extend to three years and with fine which may extend five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Under Section 67 (A) : Punishment for publishing or transmitting of material containing sexually explict etc in electronic form, who ever conduct this shall be punished first conviction for a term which may extend to five years and with fine which may extend to ten lakh rupees in the event of second conviction with imprisonment of a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Under Section 67 (B) : Punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form – whoever conduct or explicit this act shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Under Section 67 (C) : Any intermediary knowingly contravenes the provisions of sub section (I) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

WHAT OFFENCES ARE COVERED UNDER THESE LAWS ?

Hacking : It is not defined in either IT Act, which in itself may have considerably weakened the cyber crime legislation in India.

Data theft : This offence is defined as copying or extracting information from a computer system without the owners, including computer theft and theft of digital signals during transmission.

Identify theft (including password theft) : As per the IT Act 2008, this offence is defined as fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of a person.

Email spoofing : This is commonly used by hackers to hide the actual email address from which phishing and spam message are sent, it may also be used in conjunction with other fraudulent methods to trick users into providing personal confidential information.

Sending Offensive Messages : The IT Act defines this offence as sending offensive or false information for the purpose of causing hatred, ill will etc.

Voyeurism : This is defined as publishing / transmitting of "Compromising" images / videos of a person without his / her consent.

Child Pornography : This covers offences against all individuals who have not completed 18 years of age. Despite being one of the most serious offences, it does not attract any severe punishment.

Cyber Terrorism : The addition of this offence was a major difference between the two IT Acts. Cyber terrorism is described in fair detail as denying access to a computer, attempting to access a computer resource without authorization, or contaminating a computer system.

TYPES OF CYBER CRIME :

Hacking with Computer System :-

Whoever with the internet 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 an information residing in a computer resource or diminishes its value of utility or affects it injuriously by any means, commits hacking. Various techniques used by hackers which are below.

SQL Injections : An SQL injection is a technique that allows hackers to ply upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL data base. This process involves entering portions of SQL code into a web from entry field most commonly username and password. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

Theft of FTP Passwords : This is another very common way to tamper with websites. The thief search the victim's system for FTP login details and then relays them to his own remote computer. He then logs into the website via the remote computer and notified the web pages as he or she pleases.

Cross Site Scripting : This is also known as XSS, It is very easy way of circumventing a security system. In a typical xss attack, the hacker infects a webpage with a malicious client side script or program.

Virus dissemination :

Viruses are computer programs that attach themselves to infect a system or files and have a tendency to circulate to other computer on a network. They disrupt the computer operation and affect the data stored either be modifying or by deleting it altogether. Computer viruses usually spread through internet or removable media.

Logic Bombs :

A logic bomb also known as slag code, is a malicious pice of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It is not a virus, although it usually behaves in a similar manner.

Logic bombs are usually employed by disgruntled employees working in the IT sector.

Denial – of – service attach :

Using this technique, the attacker can render a website inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. A denial of service attacks violates the acceptable use policies of virtually all internet service providers.

Phishing :

This is a technique of extracting confidential information such as credit card numbers and username password.

Email bombing and spamming :

This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam fitters.

Web Jacking :

Web jacking devices its name from vijacking. The hacker taks control of a web site fraudulently. He may change the content of the original site. The owner of the website has no more control and the altacker may use the website for his own interests.

Cyber Staking :

Cyber stalking is a new form of internet crime in our society. A cyber stalker does not physically follow his victim. The cyber stalker virtually following online activity to harvest the information of stake. Most victim of this crime are women who are stalked by men and children.

Data diddling :

This is one of the simplest methods of committing a computer related crime because even a computer armature can do it.

Software Piracy :

Software piracy is the unauthorized use and distribution of Computer Software.

CYBER SECURITY :

Cyber security is a complex issue that cuts across multiple domains and therefore needs a set of multi dimensional and multi layered structures. It also requires the government to think and act as a single entity even though several ministries are impacted differently.

Mindful of the great vulnerability that India faces due to cyber threats at one level and the tremendous opportunity that it has to shape global dialogue.

Cyber threats take various forms including cyber warfare, cyber crime, cyber terrorism and cyber espionage. All these require a comprehensive cyber security policy that is well coordinated through a nodal authority within the country and international cooperation, preferably through conventions on cyber space out side the country.

The two best known international sources of cooperation are the united nations convention against transnational organized crime and the council of Europe's council on

cyber crime. India also has several bilateral agreements with countries like the United States and Korea.

Recent data shows that the number of cyber security incidents, including website intrusion malware, spam, virus, network scanning and probing and phishing have gone up from less than 400 in 2005 to over 13,000 by 2011.

INDO-US CYBER SECURITY CO-OPERATION :

India and the US have signed an accord that will enable them to jointly secure their cyber spaces amid increasing attacks on sensitive records from histile elements, including terrorists. The accord on cyber security co-operation was signed between the Computer Emergency Response Teams (CERT-IN and US-CERT) the lead agencies in the respective countries to respond to virtual attacks. The CERT-IN functions under the ministry of communication and iT and its primary role is to raise security awareness among India's cyber community and to provide technical assistance and advise them to recover from computer security incidents. The US-CERT is the operational arm of the National Cyber security Division in the Department of Home Land Security.

As per the accord, the two countries will now be able to share expertise in artifact analysis like studying traces of virus and worm, network traffic analysis and exchange of information. Though attack from hackers – professional or amature – can come from any where in the world, cyber onslaughts on Indian websites have been more frequent from China and Pakistani hackers peeking into India's sensitive business, security and strategies records. The nature of cyber attacks becomes more complex due to rapid change hackers put in place.

PUBLIC PRIVATE PARTNERSHIP (PPP) FOR CYBER SECURITY :

National Security Adviser Shivshankar Menon recently opened up the National security regime to the private sector, with the lunch of a cyber security report titled "Recommendations of Joint Working Group on Engagement with Private Sector on Cyber Security. The enormous potential for damage has made cyber security a major concern. There is no question that both the government and private sector need each other. The unique nature of this collaboration is because of the unique nature of the domain. Referring to the recent spate of riots in Uttar Pradesh, Assam and Mumbai, Mr. Menon pointed towards the misuse of social media to affect communal harmony. The challenge lies in creating a virtuous circle of security while maintaining our democratic rights of freedom of speech and privacy. Deputy NSA Vijay Latha Reddy, has been leading the initiative from its conception. At the lunch of the report, she stated that the primary objective of creating a permanent mechanism for public –private partnership (PPP) in the area of cyber security is to eventually establish India as the global hub for cyber security services, products and manpower. She also pointed out the need for a mind boggling five lakh professionals to protect cyberspace. The available talent is just a fraction of this , necessitating a rapid scale up of capacities. According to the cyber security report, collaboration is invited across four issues : the setting up a permanent JWG under the aegis of National Security Council Secretariat (NSCS), with representatives from Government and Private Sector, a permanent advisory committee called 'Joint committee on International co-operation and Advocacy to promote India's National Interests at various international for a, and information sharing and analysis centres in various sectors to cooperate with computer emergency response teams at the operational level. The composition of these working groups will be finalized in consultation with industry associations.

FINDING FROM THE STUDY :

Computer is a machine which obeys the orders of the user therefore fault lies with the user not with the Computers. The computer is a boon or a bane depends on its use. A cyber crime is a virus program that can modify another program in deemed

infected. This can also become an evolved copy of the original virus program. Every program that gets infected may also act as a virus and thus the infection multiplus. The key property of a virus is its ability to infect other programs. Every general purpose system currently in use is open to viral attack in some secure systems, virus tends to spread further when created by some user of the system. A virus has the potentials to spread throughout any system which allows sharing. The virus can be generated and introduced by a hacker. The perpetrator gets the satisfaction of demonstrating human superiority over a cybermetic system. The most fundamental precaution against virus attacks is to limit access to a machine to avoid tamper with the system.

HOW TO SOLVE THE PROBLEM OF CYBER CRIME :

Cyber Forensics is basically the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Cyber Forensic is the use of technology and science for investigation and fact recovery when dealing with criminal matters. Computer forensics is the technological aspect of retrieving evidence to use within criminal or civil courts of Law.

SUGGESTION:

The following prevention shall be implemented to safe guard the cyber crime of computers and computer information system.

Proper placement and installation of information technology equipment to reduce the effects of interference due to electromagnetic emanations.

Only authorized and legal software shall be used on the network.

The suitability of new hardware, software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.

Organisation shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorized access, loss of and damage to information outside normal working hours.

Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

System programmers shall not be allowed to have access to the application system's data and programme files in the production environment.

Certain minimum quality standards for password shall be enforced.

Passwords shall always encrypted in storage to prevent authorized disclosure.

For computer system processing sensitive data, access by other organizations shall be prohibited or strictly controlled.

The use of user IDs for emergency use shall be recorded and approved. The password shall be rest after use.

After maintenance, any exposed security parameters such as passwords, user IDs and account will be changed or rest to eliminate and potential security exposures.

All floppies should be scanned individually and periodically by using a qualified and uninfected virus scanning (or detection) program.

Discourage the use of floppies of other users unless these are individually scanned and checked for any virus.

Do not use previously formatted floppies brought by others even if these are apparently empty. Reformat all empty floppies with your uninfected system before further use.

Avoid lending floppies.

Use of pirated software should be completely avoided as most of them are virus carriers.

It the compute system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system operators or users shall scan the computer system and its devices.

User should also have some basic knowledge about viruses, their prevention and cure. Use of good antivirus software for scanning files regularly should be used by every user.

CONCLUSION :

Now India's position become pivotal on the global cyber security dialogue is its over 800 million mobile subscribers and a targeted half – a – billion internet users, who could contribute (Rs.5 Lakh crore) to India's GDP by 2015 as per a report that will soon be released by global management consulting firm me Kinsey. Equally, India's IT and BPO industry, which is expected to cross (Rs. 5 Lakh crore) in 2012 with export revenue $69.01 billion, is in the business of software development and outsourcing contracts for large global corporations and governments, making India's cyber security a matter of deep concern for global companies and western governments alike. India is now taking on the issues of cyber security to enhanced cooperation with international governments towards cyber security strategy.

REFERENCES

Advanced Computing : An InternationalJournal (ACIJ)., No.6, November- 2011.

Atul Jain (2005), Cyber Crime : Issues, Threats and Management, Pub : Isha Book Publishing House, New Delhi.

A.K. Pore, A.S. (1999) : Free expression in age of Internet : Social and Legal boundaries, Pub – Boulder, West Vie Press, USA.

Bawa Sukhminder, Mand H.S., Sharma Suraj (2008) Fundamentals of Information Technology and MIS, Pub – Kalyani Publishers, New Delhi – 110002

Chroncle – Journal – October 2012.

Chroncle – Journal – December 2012.

Dr. B. Muthukumaran, Chief Consultant, Gemini Communication Ltd., Cyber Crime Scenario in India.

Forder. Jay (2001), Electronic Commerce and the Law, Pub : John Wiley and Sons, Singapore-2001.

First Track to Cyber Crime, Pub – Journal "digit", Vol-7- issue December, 2012.

King David (1992) Project Management made simple : A Guide to successful management of Computer System Projects.

Kaur Amandeep, Gill Gurpreet (2009) Analog Communication System, Pub – Kalyani Publishers, New Delhi – 110002.

Kaurmanpreet (2012) : - Internet Application, Pub - Kalyani Publishers, New Delhi – 110002.

Mishra R.C (2005), Cyber Crimes : Impacts in the New Millennium, Pub : Authorspress, New Delhi.

PerriH. Henry (1996), Law and the Information Superhighway, Pub : Aspen Law Publishers, USA.

Phillips, Dwayne, The Software Project Managers Handbook (IEE Computer Society,2000)