The Seybold Report

ISSN 1533-9211

CYBER SECURITY LAW AND POLICIES IN INDIA

SONIYA DHANTOLE

Research Scholar (Law) School of Law and Legal Study, Sanjeev Agrawal Global Educational University Bhopal (M.P.).

Dr. SUNIL KUMAR PANDEY

Dean, School of Law and Legal Study, Sanjeev Agrawal Global Educational University Bhopal (M.P.)

Abstract

The internet is one of the greatest invention ever in the history of mankind. Internet has evolved into a virtual world where almost everything is available at the click of a button. Yes, almost everything. Everything has twos attached to itself- good and bad it always depends on which side you want to be. Hence, there arises a need for cyber laws to tackle cyber-crime cases. Cybercrime can involve criminal activities that are traditional in nature. Such as theft, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are address by Information Technology Act 2000. Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided, the truth is that the criminals have changed their method and have started relying of the advanced technology, and in order to deal with them the society, the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further the experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can efficiently fight the cyber criminals. Thus, necessary facilities must be established in various parts of the country so that crime in the virtual world can be contained.

INTRODUCTION

Cybercrime is not defined in Information Technology Act 2000 or in the IT Amendment act 2008 or in any other legislation in India. In fact it cannot be too. A general definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both"[1]. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cybercrime, we can say, it is used to describe a range of offences including traditional computer crimes, as well as network crimes. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cybercrime if the basic data or aid to such an offence is a computer or information stored in a computer used by fraudster. The Information Technology Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime. In a cybercrime, computer or the data itself the target or the object of offence or a tool in committing some other offence. All such acts or crime will come under the broader definition of cybercrime. Other words represents the cybercrime as "criminal activity directly related to the use of computer specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment"[2]. The internet space or cyber space is growing very fast and as the cybercrime.

The Seybold Report
ISSN 1533-9211

Types of Cyber Crime

1. **Hacking:** - A hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an invasion into the privacy of data. There are different classes of Hackers.
   a) **White Hat Hackers: -** They believe that information sharing is good and that it is their duty to share their expertise by facilitating access to information. However, there are some white hat hackers who are just "joy riding" on computer system.
   b) **Black Hat Hackers:** - They cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are called 'crackers'.
   c) **Gray Hat Hackers: -** Typically ethical but occasionally violates hacker ethics hackers will hack into network, stand-alone computers access to private computer network just for challenge, curiosity and distribution of Information.
2. **Software Piracy:** - It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copyright and a violation of license agreement.
3. **Cyber pornography:** - Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attack children to such funs. Later they are sexually exploited for gains.
4. **Spamming: -** Spamming is sending of unsolicited bulk and commercial message over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers.
5. **Phishing: -** It is a criminally fraudulent process of an acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.
6. **Cyber Stalking: -** This crime involves use of internet to harass someone. This behavior includes false accusations, threats etc.
7. **Password Sniffers: -** Password sniffers are programs that monitor and record the name and password of network users as they log in jeopardizing security at a site.
8. **Cyber Terrorism: -** The use of computer resources to intimidate or coerce Government, the civilian population or any segment thereof in furtherance of political or social objections is called cyber terrorism.
9. **Web jacking:** - The term refers to forceful talking of control of a web site by cracking the password.
10. **Credit Card Fraud:** - In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line data base.

The Seybold Report
ISSN 1533-9211

11. **Corporate Espionage:** - IT means theft of trade secret through illegal means such as wiretap or illegal intrusions.
12. **Embezzlement: -** Unlawful misappropriation of money, property or any other thing of value that has been entrusted to the offenders care, custody or control is called embezzlement.
13. **Money Laundering: -** It means moving of illegally acquired cash through financial and other system so that it appears to be legally acquired.
14. **Spoofing: -** It is the act of disguising are computer to electronically "look" like another computer, in order to gain access to a system that would be normally is restricted.

International Dimensions of Cyber Crime

Cybercrime often has an important dimensions. E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient or illegal content is stored outside the country. There are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role. One example is illegal content. The criminalization of illegal content differs in various countries. In terms of illegal content, internet users can access information available legally abroad, that could be illegal in their own country. Theoretically, developments arising from technical standardization go far beyond the globalization of technology and services and could lead to the harmonization of national laws. The computer technology currently in use is basically the same around the world. Apart from the language issues and power adopters, there is very little differences between the computer system and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the internet. Due to standardization, the protocols used in countries on the African continent are the same as those used in the United States. Standardization enabled users around the world to access the same services over the internet. The internet does not recognize any border control, but there are means to restrict access to certain information. The drafter of the standford Draft Convention[3] recognized the importance of the international dimension of cybercrime and the related challenges. In order to address these challenges they incorporated specific provisions that deal with international cooperation. The provisions cover the following topics:

- Article 6 – Mutual Legal Assistance.
- Article 7 – Extradition.
- Article 8 – Prosecution.
- Article 9 – Provisional Remedies.
- Article 10 – Entitlements of an Accused person.
- Article 11 – Cooperation in Law Enforcement.

This approach shows a number of similarities to the approach taken in the convention of cybercrime.

The Seybold Report
ISSN 1533-9211

Statutory Provisions

The Parliament of India considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act 2000 was passed and enforced on 17th may 2000. The preamble of the Act states that its objective to legalize e-commerce and further amend the Indian Penal Code 1860, The Indian Evidence Act 1872, the Banker's Book Evidence Act 1891 and the Reserve bank of India Act 1934. The basic purpose to incorporate the change in this Acts is to make them compatible with the Act of 2000.So that they may regulate and control the affair of the cyber world in an effective. The Act Also provide legal recognition carried out by means of electronic communication. The Act deals with the law relating to Digital contracts, Digital property and Digital Rights. Any violation of these laws constitutes a crime and it prescribes very high punishments.

The Information Technology (Amendment) Act 2008 (Act 10 of 2009), has further enhanced the punishment. Life imprisonment and fine up to rupees ten lakhs may be given for certain classes of cybercrimes. Compensation up to rupees five crores can be given to affected person if damage is done to the computer, computer system, or computer network by the introduction of virus, denial of services etc. [Sec.46(1-A)]. Sections 65 to 74 of the Act specifically deals with certain offences related to cybercrimes.

Cyber Terrorism and National Security in India

Crime is a social and economic phenomenon and is as old as the human society. It is the legal concept and has the sanction of the law. Crime means any conduct accompanied by act or omission prohibited by law so crime and offence is a legal wrong that can be followed by criminal proceeding which may result into punishment.

Cyber terrorism is emerging as a very serious threat in today's world. The internet brings joy to our lives but at the same time it has some negative sides too. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims.

Today everybody is using the computers example white collar employees to terrorist's and from teenagers to adults. Infect the new generation is growing up with computers and most important is that all the monitory transactions are moving on to the internet so it has become very important to us to be aware of the various cybercrimes being committed with the help of computer. The national research council, *"Computers a Risk"* 1991 has stated.

"The modern thief can steal more with a computer than with a gun. Tomorrow's Terrorist may be able to do more damage with the key board than with the bomb".

By using the internet the terrorist can affect much wider damage or change to the country than one could by killing some people. From disabling the countries, military and defences to shutting off the power in all large area. The terrorist can affect more people at less risk to him, or herself, then through other means.

The Seybold Report
ISSN 1533-9211

Cyber terrorism takes many forms. One of the more popular is to threaten a large bank. But the one measure a problem of the countries is that to the difficulty to catch the criminals is that the criminals may be in other countries.

A second difficulty is that most banks would rather pay the money than have the public know how vulnerable they are some examples of cyber terrorism in its many form.

Case 1.

Cyber terrorist often commit acts of terrorism simply for personal gain. Such a group, known as the chaos computer culb, was discovered in 1997. They had created an Active X Control for the internet that can trick the Quicken accounting program into removing money from a user's bank account. This could easily be used to steal money from users all over the world that have the Quicken software installed on their computer. This type of file is only one of thousands of types of viruses that can do everything from simply annoy users, to disable large networks, which can have disastrous, even life and death, results.

Case 2.

Minor attacks come in the from of "data diddling", where information in the computer is changed. This may involve changing medical or FINANCIAL records or stealing of passwords. Hackers may even prevent users who should have access from gaining access to the machine. Ethical issues in this case include things like invasion of privacy and ownership conflicts. It could be even more serious if, for instance, the person who needed access to the machine was trying to same someone's life in a hospital and couldn't access the machine. The patient could die waiting for help because the computer wouldn't allow the necessary access for the doctor to save his or her life.

Weapons of Cyber Terrorism

(a) Hacking: Some ingredient technologies like packet sniffing, tempest attack, password cracking and buffer outflow facilitates hacking.

(b) Trojans: Programmes which pretend to do one thing while actually they are meant for doing something different.

(c) Computer Viruses: It is a computer programme, which infect other computer, programmes by modifying them. They spread very fast.

(d) Computer Worms: The term 'worm' in relation to computers is a self is self-contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connection.

(e) E-mail Related Crime: Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.

(f) Denial of Service: These attacks are aimed at denying authorised persons access to a computer or computer network.

The Seybold Report
ISSN 1533-9211

(g) Cryptology: Terrorist have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

Existing Cyber Security

1. National Informatics Centre (NIC).
2. Indian Computer Emergency Response Team (Cert-In).
3. National Information Security Assurance Programme (NISAP).

Prevention of Cyber Crime:

1. Children should not give their identifying information such as their name, home address, school name, phone number in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive. They should remember that people online might not be who they seem.
2. Parents should use content filtering software on their comlputers so that their child is protected from the pornography, gambling drugs and alcohol. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.
3. Keep back-up volumes so that one may not suffer data loss in case of virus contamination.
4. Always use latest and update anti-virus software to guard against virus attacks.
5. Never send your credit card number to any site which is not secured.
6. Do not panic if you find something harmful. If you feel any immediate physical danger, contact your local police. Moreover avoid getting into huge arguments online during chat and discussions with other users. Be careful about personal information about yourself online.

Judicial Decision on Cyber Crimes

Avnish Bajaj vs. State (N.C.T.) of Delhi,[4] In this case, Avnish Bajaj, CEO of Baazee com., an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee. Com website.

The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1lakh each. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the court and also ordered to participate and assist in the investigation.

Syed Asifuddin and Ors Vs. The State of Andhra Pradesh &Anr,[5] Tata Indicom employees were arrested for manipulating of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

The court held that such manipulation amounted to tampering with computer source code as envisages by Section 65 of the Information Technology Act 2000.

The Seybold Report
ISSN 1533-9211

State vs. Mohd. Afzaland others[6], several terrorists had attacked the parliament house on 13th December, 2001. Digital evidence played an important role during this prosecution. The accused had argued that computers and Digital evidence can easily be tampered and hence should not be relied upon.

The court dismissed these arguments. It said that challenges to the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation, should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Firosvs. State of Kerala[7]**,** The Government of Kerala issued a notification U/S 70 of Information Technology Act declaring the FRIENDS (Fast, Reliable, Instant, Efficient Network for Disbursement of Services) application software as a protected system.

The author of the application software filed a petition in the High Court against the said notification. He also challenged the constitutional validity of Section 70 of Information Technology Act.

The court held that there is no conflict between the provision of Copyright Act and Section 70 of IT Act and Sec. 70 of IT Act is not unconstitutional. While interpreting Sec.70 of IT Act, a harmonious construction with copyright Act is needed. Sec.70 of IT ACR is not against but subject to the provision of the Copyright Act.

State of Tamil Nadu Vs. SuhasKatti[8]**,** This case concernedthe porting of obscene, defamatory and annoying messages about a divorcee women in the Yahoo! Message group. The perpetrator also forwarded emails to the victims for information through a false e-mail account who had opened in her name. The women got annoying phone calls from people who were under the misapprehension that she was soliciting. The accused was arrested and found guilty of offences under Sections 469, 529, of Indian Penal code and Section 67 of Information Technology Act 2000 and was successfully convicted and sentenced for offence.

Nassacomvs. Ajaysood& Others,[9] The Delhi High Court declared phishing to be an illegal act entailing an injunction and the recovery of damages. The court laid down the ambit of phishing and declared it to be a form of internet fraud where a person pretended to his advantage to be a legitimate association like a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords etc.

Diebold System Pvt. Ltd. vs. Commissioner of Commercial Taxes,[10] It is an interesting case, the Karnataka High Court laid down that ATMs are not computer, but are electronic devices under the Karnataka Sales Tax Act, 1957.

Diebold system Pvt. Ltd.[a manufacturer of and supplier of Automated Teller Machine (ATM) had sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 on sale of ATM.

The majority view of ARA was to classify ATMs as “computer terminals” liable for 4% basic tax as they would fall under Entry 20(ii)(b) of part ‘C’ of Second Schedule to the Karnataka Sates Tax Act.

The Seybold Report
ISSN 1533-9211

The chairman of ARA dissented from the majority view. In his opinion, ATMs would fit in to the description of electronic goods, parts and accessories thereof. They would thus attract 12% basic tax and would fall under Entry 4 of part 'E' of the Second Schedule to the KST Act.

The commissioner of Commercial Tax was of the view that the ARA ruling was erroneous and passed an order that ATM cannot be classified as computer terminals.

The High of Karnataka acknowledged that the IT Act provided an enlarged definition of "computers". However the court held that such a wide definition could not be used for interpreting a Taxation related law such as Karnataka sales Tax Act, 1957.

The High Court also said that an ATM is not a computer by itself and it is connected to a computer that performs the tasks requested by a person's using the ATM. The computer is connected electronically to many ATMs that may be located at some distance from the computer.

State Bank of India vs. Rizvi Exports Ltd.[11] State Bank of India had filed a case to recover money from some persons who had taken various loans from it. As part of the evidence, State Bank of India submitted printouts of statements of accounts maintained in State Bank of India's computes system.

The relevant certificates as mandated by the Bankers Books of Evidence Act (as amended by Information Technology Act) had not been attached to these printouts. The court held that these documents were not admissible as evidence.

R vs. Boden[12], a 49 years old hacker, VotekBoden was sentenced to two years' imprisonment after being found guilty of hacking into the Maroochy Shire's computerized waste management system. Boden was accused of causing millions of liters of raw sewage to spill out into local rivers and park killing marine life and causing offensive smells. He was apparently motivated by revenge after having been refused a job at a plant.

Impacts of Cyber Crime

1. Potential Economic Impact:-

The 2011 Norton cybercrime disclosed that over 74 million people in the United States were victims of cybercrime in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cybercrime resulting in 1 million cybercrime victims a day. Many people have the attitude that cybercrime is a fact of doing business online[13]. As today's consumer has become increasingly dependent on computers, networks and the information these are used to store and preserve, the risk of being subjected to cybercrime is high. Some of surveys conducted in the past have indicated as many as 80% of companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $50 million. Almost 10% reported financial fraud[14]. As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber criminals.

The Seybold Report
ISSN 1533-9211

2. Impact on Market Value:-

The economic impact of security is of interest to companies trying to decide where to place their information security budget as well as for insurance companies' that provide cyber- risk policies[15]. Recently, some insurance companies' tables that they believe provide ways to measure losses from computer interruptions and hackers attack. However, these estimates are questionable mostly due to the lack of historical data.

3. Impact on Consumers Trust:-

Since cyber- attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognize as the root cause. This makes the customer lose confidence on the said site and in the interest and its strength. According to report sponsored by the Better Business Bureau Online, over 80% of online shopper cited security as a primary worry when conducting business over the internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception that the internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce.

Reasons for Cyber Crime

Hart in his work "The Concept of Law" has said," human being are vulnerable, so rule of law is required to protect them". Applying this to the cyberspace it may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber-crime. The reason for vulnerabilities of computers may be said to be –

1. **Capacity to store data in comparatively small space**: - The computer has unique characteristics of storing data in a very small space. This affords to remove or drive information either through physical or virtual medium makes it much easier.
2. **Easy to access**: - The problem uncounted is guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to complex technology.
3. **Negligence**: - Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber-criminal to gain access and control over the computer system.
4. **Loss of evidence:** - Loss of evidence is very common and obvious problem as well as the data are routinely destroyed. Further collection of data outside the territorial extent also paralyze this system of crime investigation.
5. **Complex:** - The computer work on operating system and these operating system in turn are composed of millions of codes. Human mind of fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the complex system.

The Seybold Report
ISSN 1533-9211

Prevention of Cyber Crime

Prevention is always better than cure.it is always better to take certain precaution while operating the net. SailashkumarZarkar, technical advisor and network security consultant to the Mumbai Police Cyber Crime Cell, advocates the 5P mantras for online security; precaution, protection, protection, preservation, and preservance. A citizen should keep in the following things -

1. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
2. To prevent cyber stalking avoid disclosing any information pertaining to oneself.
3. Always use latest and update anti-virus software to guard against virus attack.
4. Never send any credit card number to any site that is not secured, to guard against frauds.
5. It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

Present Scenerio of Cyber Crime

In the present global situation where cyber control mechanism are important we need to push cyber laws. Cyber-crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber-crime. The seven stage continuum of a criminal case starts from to preparation, to registration, to reporting, to investigation, to prosecution, to adjudication, and to execution. The system cannot be stronger than the weakest link in the chain. The increasing use of technology, particularly by business to drive its operations and to deliver world class services has led to the evolution of a new threat. The growth of complexity and access to technology has made us more susceptible to 'hi-tech crime' which is also a new forum of business threat that requires a fundamental shift in risk management arena of business, particularly in the financial domain where the risk is very high. In India, 59% of mobile phone owners access internet via mobile device out of which 17% experienced mobile related cybercrime[16].One recent ranked India in 2008 as the fourteenth country in the world hosting phishing websites[17]. Seriousness could be ascertained from the report published by the world Economic Forum: Global Risks 2012 in which cyber threat is rated as serious threat to the world based on likelihood of impact cyber threats are real and its impact could be felt across border, business and communities.

In India, there are30 million policeman to train apart from 12,000 strong judiciary. Police in India are trying to become cyber-crime savvy and hiring people who are trained in the area. Each police station in Delhi will have a computer soon which will be connected to the Headquarter. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and distinct judiciary. IT Institutes can also play a role in this area.

The Seybold Report
ISSN 1533-9211

CONCLUSION

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided, the truth is that the criminals have changed their method and have started relying of the advanced technology, and in order to deal with them the society, the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further the experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can efficiently fight the cyber criminals. Thus, necessary facilities must be established in various parts of the country so that crime in the virtual world can be contained[18]. Today cyber-crime is no longer the domain of high school hacker but is populated by organized criminals, unfriendly nation stated and terrorists. The problems we face are far more physical security is threatened by vulnerabilities in our electronic information system.So, the law cannot afford to be static; it has to change with the changing times. The bottom – line is that law should be made flexible so that it can easily adjust to the needs of the society and the technological development.

Footnotes

1) Nagpal R. --- What is Cyber Crime?
2) Wow Essay (2009), Top Lycos Networks.
3) The Standford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Standford University in the United States in 1999. The text of the convention is published in: The Transnational Dimension of cybercrime and Terror, Page249 et seq.
4) (2005)3 compLJ364 (Del), 116(2005)DLT427, 2005(79)DRJ576
5) 2005 criLJ314 (AP).
6) 2003 VIIAD (Delhi)1, 107(2003)DLT385, 2003(71)DRJ 178, 2003(3)JCC1669
7) AIR 2006 ker 279, 2006(3) KLT 210, 2007(34) PTC98 (Ker).
8) CMM, Egmore, Chennai in 2004.
9) 2005(30) PTC 437.
10) ILR 2007 KAR 2210, [2006]144 STC 59 (kar)
11) II (2003) BC 96.
12) [2002] QCA 164
13) Kevin G. coleman (2011), cyber intelligence: The Huge Economic impact of Cyber Crime.
14) PTI contents (2009), Indian: A Major hub for cybercrime.
15) Gordon L. A. et al., 2003, A Framework for using Insurance for cyber-Risk Management, Communications of the ACM 46(30: 81-85.
16) Symantec Cyber Crime Report 2011.
17) India emerging as major cyber crime Centre (2009).
18) Cyber cell of the law enforcement agencies have started operating in Metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc.

The Seybold Report
ISSN 1533-9211

Bibliography

Books Referred:

1) Lalithashidhar: Cyber Crimes and Real World Society.
2) Talwant Singh, Addl. Distt. & Session Judge, Delhi: Cyber Law and Information Technology.
3) Rahul Matthar: Law Relating to Computers.
4) M. K. Bhandari: Intellectual property Right.
5) Narayan: Indian Copyright Laws.

Journals Referred:

1) Indian Law Report 2007.
2) Criminal Law Journal 2005.
3) Symantec Cyber Crime Report 2011.

Cases Referred:

1) Vanish Bajaj vs. State(N.C.T.) of Delhi, (2005)3 compLJ364 (Del), 116(2005)DLT427, 2005(79) DRJ576
2) Syed Asifuddin and vs. the State of Andhra Pradesh &Anr, 2005 criLJ314 (AP).
3) State vs. Mohd. Afzal& Others, 2003 VIIAD (Delhi)1, 107(2003)DLT385, 2003(71)DRJ 178, 2003(3)JCC1669
4) Firos vs. State of Kerala, AIR 2006 ker 279, 2006(3) KLT 210, 2007(34) PTC98 (Ker).
5) State of Tamil Nadu vs. SuhasKatti,CMM, Egmore, Chennai in 2004.
6) Nassacom vs. Ajay sood& others,2005(30) PTC 437.
7) Diebold System Pvt. Ltd. vs. Commissioner of Commercial Taxes,ILR 2007 KAR 2210, [2006]144 STC 59 (kar)
8) State Bank of India vs. Rizvi Exports Ltd.,II (2003) BC 96
9) R. vs.Boden,[2002] QCA 164