International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-10, Issue-3 May-June-2023
P-ISSN 2349-1817
www.ijesrr.org
Email- editor@ijesrr.org

Impact of Social Transformation on Cyber Laws

Ms. Shreya Agarwal

Abstract

Commenting on the information technology progress which has transformed the world into a global village. The technology has made us a 'global Village[1]' in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated in our society. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long"[2].

1. Introduction

"Bits and bytes are replacing bullets as well as bombs in the world Crime[3]". The growth of cyber crime in India and all over the world, is on the rise and to curb its scope and complexity is the pertinent need today. Cyber space offers a plethora of opportunities for cyber criminals either to cause harm to innocent people, or to make a fast buck at the expense of unsuspecting citizens.

Every walk of life we getting exposed to cyber crime. Several people have come forward and reported such crimes, which have met with an assuring and prompt response from the law enforcement authorities from the different cities of the country.

The practice of any craft builds expertise and excellence over a period of time, and the nascent field of cyber crime investigation is no exception. It is clear that in India, this building of a community practice has started happening and the cyber sleuths are learning new tools and honing them with initiative and experience.

The advancement of technology has brought about radical changes in the modern society. But human experience has shown that every technological change brings with it some unforeseen problems, taking advantage of which the law breakers explore new techniques to perpetrate their criminal activities.

In fact, technology-generated crimes not only affect individuals or a nation, but have a widespread ramification throughout the world. Internet is one such gray area, which has given rise to the menace of cybercrimes.

*** Assistant Professor, Mewar Law Institute, Sector 4C-Vasundhara, Ghaziabad, UP-201012.**

[1] Walter.B.Wriston, The Twilight of Sovereignty : How the Information Technology Revolution is Transforming Our World (2003) p.31.

[2] Supra.1

[3] John Naugent,Texas Woman,s University,DOI:10.4018/9781591409915.ch004

The computer based global communication system has crossed the territorial borders thus creating a distinct field for online criminal activity warranting global attention.

2. Meaning of "Cyber" vs-a-vs Cyber Crime

"Cybercrimes" have emanated from development of computer network. Internet in the present millennium has become all pervasive and omnipresent. It has also brought with it new problems hitherto unknown to humanity. Internet in a sense is analogous to the "high seas" which no one owns yet people of all the nationalities use it. The term 'cybercrime' encompasses within it a variety of criminal activities taking place in the cyberspace through the media of global communication via internet. It is an inevitable evil having its origin in the growing dependence of mankind on computers in modern life, the reason being that the computers despite being high technology devices are extremely vulnerable.

Thus, whenever any crime or criminal activity takes place with the use of computer, it constitutes a cybercrime. It is for this reason that 'cybercrime' has been defined as "an unlawful act wherein the computer is either a tool or a target or both".

The foregoing analysis clearly indicates that cybercrimes are such harmful activities in the cyberspace which may cause damage to a person, property or even the State or society as a whole.

3. Evolution of Information Technology Act in India

The menace of cyber criminality is not confined to one or two countries but the whole world is facing this gigantic problem as a "technological scorn". India is no exception to this computer generated menace. However, as a measure to prevent and control internet crimes, legislation enacted the Information Technology Act, 2000 which came into force on October 17, 2000.

The Act categorically defines offences relating to cyberspace such as tempering with computer source document, hacking with computer system, breach of confidentiality and privacy etc.It is not that prior to this legislation there was no law to deal with these offences. The Indian Penal Code, 1860 already contained provisions to prevent and control cybercrimes but they were not found to be sufficient enough to tackle all varieties of cyberspace crimes. The obvious reason being that no one knew about the computer or internet[4] at the time when the Indian Penal Code was enacted.

It hardly needs to be stated that science and technology has extended its tentacles cutting across the national frontiers whereas the law is still struggling to define and redefine the boundaries for the control of cybercrimes.

[4] The computer technology has mainly developed and expanded throughout the world only during the last quarter of 20th Century

Cybercrime being global in character, generally affects the person far away from the place of offence, may it be in the same country or some other country. It therefore, requires policing at international level as also the active cooperation of the international community.

4. Effects of UN Convention

The European Convention on Cybercrime[5] was indeed a praiseworthy attempt as it laid down guidelines to be followed by the member States in combating cybercrime. The Convention suggested measures to be initiated by the states for restructuring their cyber laws to meet the new challenges. The Convention not only dealt with the changes and improvements in the substantive part of criminal law but also referred to the procedural aspect which must be taken into consideration while restructuring the existing law to meet the current needs of developing technology.

Out of a variety of cybercrimes, the European Convention has chosen ten specific cybercrimes[6] and urged the member States to include them in their information technology laws and provide a concrete mechanism to fight against them. But it is rather unfortunate that many cybercrimes of a particular country are not treated as crime under the criminal law of other countries, which really poses a problem when cross country cybercrimes are involved.

The solution to this problem lies in enacting a global cyber law uniformly applicable to all the countries of the world. In other words, uniformity be ensured with reference to substantive cyber laws of various nations.

A nation wise survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many of them have not even initiated steps to frame laws for policing against these crimes. This divergent approach of world nations towards the desirability of cyber law poses a real problem in handling the internet crime and at the same time provides ample scope for the cyber criminals to escape detection and punishment.

All the nations should therefore, realise the need and urgency for generating awareness about the dangerous nature of cybercrimes which are perpetuating illegal online activities in cyberspace. Cyber criminality is perhaps the deadliest epidemic spread over the world in the new millennium which has to be curbed by adopting a global preventive strategy[7].

So far India is concerned, it has introduced a comprehensive information technology law by amending the Principal Information Technology Act, 2000 by the I.T. (Amendment) Act, 2008 w.e.f 5th February, 2009. The amending Act has inserted as many as 15- new cyberspace offences which are punishable under the I.T.

[5] Effective From June, 2001
[6] Section 1, Chapter II of the European Convention document which contains Articles 2 to 13 defining ten cybercrimes under five separate titles
[7] The Information Technology Act, 2000 which came into force w.e.f. October 17, 2000.

Act. That apart, many of the provisions of the Indian Penal Code have been amended to include within it certain criminal acts relating to cyberspace and electronic media.

Broadly speaking, the law enforcement agencies all over the world are confronted with four major problems while dealing with cybercrimes in a network environment. The detention and prosecution of cyber criminals online is hindered by the challenges, which may be technical, legal, operational and jurisdictional.

As regards technical challenges, cybercrimes such as hacking of a website, stealing data stored in computers, espionage, exchange of pornographic material, blackmailing etc. involve detection of source of communication which is a complicated task. Therefore, the cyber criminals find it easy to impersonate on the internet and hide their identity.

The legal challenge emerges from the fact that cyber criminality is no longer confined to the developed countries alone but it has assumed global dimensions in recent decades. The conventional legal techniques of investigation of cybercrimes are inadequate particularly, in case of cross-country crimes. The problem becomes more complex because of lack of any universally accepted definition of cybercrime. Therefore, a cybercrime in a country may not necessary be a crime in another country.

There are hardly twenty countries in the world which have enacted comprehensive cyber laws. In the absence of an adequate cybercrime laws, the cyber criminals carry on their illegal activities undeterred.

Therefore, effective handling of cybercrimes requires a legal framework which is equally applicable to all the countries. The cyber laws should also be responsive to the fast developing information technology. The internet has enabled the cyber offenders to target maximum number of people at a minimal cost merely at the click of a button. Therefore, cyber security assumes utmost importance.

The operational challenges faced by the law enforcement agencies because of lack of adequate cyber forensic technology for dealing with cybercrimes constitute another in-road which renders it difficult to collect and preserve sufficient evidence against the person accused of cybercrime, thereby resulting in his/her acquittal by the court.

The traditional modes of procuring evidence are unsuited in case of cybercrime investigation because most of the evidence exists in electronic form. Therefore, there is dire need to develop suitable computer forensic mechanism for effective handling by cybercrime investigation.

In the context of e-mail bombing by the Internet Black Tigers against the Sri Lankan embassies was perhaps the closest thing to cyber terrorism that has excursed so for.

Most studies to date have shown that critical information infrastructures of potentially vulnerable to a cyber terrorist attack. The increasing complexity of information systems creates new vulnerabilities and challenges

for It management. Even if the technology is armor plated, insiders acting alone or in concert with other terrorists maybe able to exploit their access capabilities to work considerable harm[8].

Computer and information security, data protection, and privacy are all growing problems. No single technology or product will eliminate threats and risk. I do not believe we have even begun to thing of the social and economics implications of a considerable cyber terrorism attack against our infrastructure. Securing our computers, information, and communications networks secure our economy and our country. A global strategy and policy for combating this type of terrorism is need now.

In fact, jurisdiction is a broad concept which refers to whether a court has the power to adjudicate, i.e., whether it has personal jurisdiction to try the case and territorial jurisdiction over the location or place where the crime is committed or the parties concerned reside. In case of cross-country cyber dispute or crime, the problem often arises as to the law of which country would be applicable to the case in hand.

5. **Net security be tightened up:**

Computer technology has proved to be a boon to the commercial world. Perhaps, it is the area which has been most benefited by the advent of computers. Most of the commercial, industrial and business transactions are carried on through internet services at the national as well as the international level. The increasing use of computers in the field of trade and commerce has at the same time opened new vistas for the perpetration of cybercrimes by the offenders for their personal monetary gain.

With the liberalization and globalization of economy, the business houses now believe that there is a huge and profitable market for commercially exploiting the networks. With the increased dependence on computer in commercial field, most of the money transactions are being carried out with the help of computer network making it possible for the cyber criminals to illegally intercept and commit financial frauds.

It is therefore, necessary that an adequate security mechanism be developed for safeguarding e-commerce and e-banking against possible online frauds, forgeries, or misappropriation of money etc.

As regards the legality of financial transaction on the internet, the Securities Exchange Board of India (SEBI) vide its notification dated January 25, 2000, has provided that trading of securities on internet will be valid in India but there is no provision to this effect in the Information Technology Act which provides legal validity and prevent security frauds and stock manipulations over the internet. A specific provision for protection of confidentiality in the net-trading, therefore, needs to be incorporated in the I.T. Act.

6. **Use of encryption technology:**

[8] Cyber Terrorism, By Kevin coleman, Technolytics, october 10, 2003 at http://www.symante.com/avcerter/reference/cyberterrorism.pdf.

It should be mandatory for all government, semi-government and non government commercial organisations which have resorted to massive computerization for the transmission of information and commercial transactions, to appoint well trained Information Security Officers who should be responsible for overall protection of computer resources and they should also be made accountable for any lapse in computer security.

The use of encryption technology may also help to protect data and communications from unlawful and unauthorised access, disclosure or alteration. It also helps to prevent crime by protecting valuable secret information over inter-connected computer and networks. The law enforcement agencies should therefore, develop and support the use of strong and recoverable encryption services for protecting personal and business data from being misused or stolen by miscreants.

Similar to encryption, there is one more technique known as 'steganography', which is used as a safeguard against network invasion. It is a technique of obscuring information in a manner so as to prevent its detection. It involves writing that is not readily discernible to the casual observer, just as in ancient times, the practice of writing secret messages in invisible ink using milk; fruit-juice or urine which darkens when heated was prevalent to transmit messages.

Firewall device is yet another tool which may be extensively used to provide an alert against attempted intrusions in database. It is a software program which monitors data flowing between one computer to another on the network. Firewall device can be used to control the amount of data flowing over one's computer network.

7. Intrusion Management:

A new preventive strategy called the 'intrusion management' may be used for testing, detection and investigation of cybercrime. It is a process which primarily aims at preventing intrusions in the computer system thus providing effective e-security control mechanism.

The computer users and e-commerce organizations should ensure that functional areas of vulnerability of the computer system are kept properly controlled so that

(i) identification and authenticity,

(ii) access,

(iii) accountability,

(iv) accuracy, and

(v) reliability of data is absolutely safeguarded.

It has been observed that most cybercrime investigations end up with the conclusion that victim's computer system has been damaged due to cybercrime attack but the source of attack could not be traced or located.

Therefore, one of the most important aspect of intrusion management is to plug the security loopholes so as to render the computer system absolutely safe and secured.

The protective measures contemplated under the intrusion management system include protection against viruses by adopting antivirus strategies, use of firewalls, authentication and encryption technology.

8. **False e-mail identity registration be treated as an offence:**

Cyber criminals often furnish fictitious information while registering themselves for an e-mail address with a website because the email service providers refuse to provide two ID's to the same person.

This false and misleading information on the internet helps the criminal to suppress his real identity and mislead the investigating authorities in reaching the real culprit. There being no provision in the Information Technology Act to prevent registration of a person for an e-mail address with a website by providing false information, a person can establish false e-mail identity with a fictitious IP address and misuse the same for perpetration of a cybercrime.

This lacunae in the Act has been taken care of by inserting a new Section 66A in the principal Act by the I.T.(Amendment) Act, 2008 (10 of 2009), which provides that any false e-mail identity registration with a website will be an offence punishable up to two years of imprisonment. It is certainly a step forward towards the prevention and control of cybercrimes.

9. **Self-regulation by computer and net users:**

Self-regulation may be suggested as one of the practicable solution to reduce the incidence of cybercrime. It is a process of developing a healthy code of conduct by adopting a policy of restraint by both, the computer users as well as the service providers. Internet Service Providers (ISP) can play a crucial role in eliminating online crimes by taking some self-regulatory initiatives.

To start with, ISPs can collectively set out a ethical code of conduct to be followed by them while extending internet services/facilities to the users. Likewise, they can lay down the conditions through a written agreement binding the users to refrain from indulging in illegal activities. Besides, they may also specify in the contract that breach of these conditions would lead to termination of the internet services.

10. **Liberalisation of law relating to search and seizure:**

Government's regulatory mechanism to control widespread cyber criminality needs to be further intensified. Most importantly, the existing legal regimes should enable the law enforcement agencies to accomplish their tasks fearlessly without any external pressure. The law-enforcement agencies should be empowered to seek such details from the Service Providers as may be necessary for the investigation of internet crime without, however, violating any of the fundamental or privacy rights of the parties.

The law relating to search, seizure and arrest as applicable to cyber-offences needs to be liberalized so as to enable the police or the investigating agencies to apprehend the cyber offenders and initiate criminal proceedings against them.

The telecommunications department should also review its policy towards ISPs and impose selective restrictions on them while extending internet services by classifying them on the basis of age, profession or standing as Internet Service Provider.

11. Use of voice-recogniser, filter software and collar-ID for Protection against unauthorised access:

Technology indeed is itself a powerful tool which has generated cybercrime. Therefore, as a first step to prevent its misuse, the places where computer is popularly used as a means for carrying out routine life activities, should be equipped with some safety and security devices to protect against unauthorised usage of computer systems.

For example, the modern voice recognition system which relies on voice pattern for activation may effectively be used. So also, anomaly detection software, which identifies unusual pattern of computer use helps the users or organisations to respond and frustrate the attacker. Similarly, filter software have afforded protection against known threats.

The use of Collar-ID technology in telecommunication as a protective measure may also help in eliminating e-mail crimes. Similar technological devices also exist to filter electronic mail from unwanted sites.

12. Development of cyber forensics and Biometric Techniques:

In order to provide substantial technical assistance to the investigating agency in identification, location, preservation and extraction of digital information from a computer system so as to produce it in the form of evidence of cybercrime before the court of law, the cyber forensic techniques need to be developed.

The cyber forensics technique consists of three components, namely, computer forensics, cyber forensics and software forensics. Obviously, the three are inter-related to constitute a compact cybercrime detection mechanism.

Computer forensics deal with collection of evidence from computer media seized at the scene of crime by extracting hidden or deleted information from the computer disk. Cyber forensics also called as ‘network forensics’, relate to digital evidence that is distributed across the large computer network.

The main object of cyber forensics is to discover the evidence and access the intent and identity of the cyber criminal as also to determine the impact of crime on the victim(s). The software forensics mainly deal with author of the malicious code and provide substantial clues to identify the perpetrator of cybercrime.

The use of computer forensics as a technique of analyzing the legal evidence would certainly facilitate cybercrime investigation and help in reaching the criminal and establishing his guilt on the basis of evidence procured and produced against him before the Court.

Like the computer forensics, the use of biometric techniques can also be of great help in identifying the real perpetrator of cybercrime.

Biometrics involves electronic analysis of attributes arising from a person's physical characteristics that are unique to that person. For example, the codes derived from electronic analysis of fingerprints, footprints, retinal scans, body odor etc. can provide important clues to identify the person accused of cybercrime, though it needs to be corroborated by other material evidence.

13. **Need to establish a Computer Crime R&D Centre:** Perhaps the most effective method of preventing cyber crime is to create awareness among the computer users about the possible dangers emanating from misuse of information technology for criminal activities.

    It is all the more necessary because every user of network is a potential victim and his ignorance about the information security and safeguards, multiplies the chances of his vulnerability to cybercrime.

    Therefore, generating awareness among the owners and users of computers through proper education may substantially help in reducing the threats as well as the damages caused by these crimes. Generally, the internet users remain unaware of the fact that while they are online, they may fall a victim to cybercrime or may themselves unknowingly involve in an activity which constitutes an offence though did they did not intend to commit it.

    This is more true particularly, in case of adolescents who, for the sake of entertainment or fun, switch over to pornographic website and sometimes themselves become a victim of such crime.

    This possibility can be eliminated by apprising the internet users about the dangers and consequences of the unlawful acts which they may inadvertently or ignorantly commit on the net.

    Some computer experts have suggested that there is dire need to set up a National Computer Crime Resource Centre with members from different segments of society such as law enforcement personnel, forensic and legal experts, computer experts, members from Central Bureau of Investigation and the Reserve Bank of India, which should collect, collate and disseminate all data relating to computer crimes among the users. The centre should also lay down a model standard procedure to ensure safe computing.

14. **Need for a Universal Legal Regulatory Mechanism:**

    Law and criminal justice delivery system have not kept pace with the technological advancements made around the world during the preceding years, which has provided ample scope for the abuse of internet.

The conventional old laws pertaining to protection of property are no longer valid for protecting the unauthorised manipulation of information through computer networks. Therefore, there is need for restructuring of the substantive as well as the procedural law relating to computer generated crimes so that offenders may be brought to justice. At present, the definition of cybercrime varies from country to country depending on the incidence of such crimes and the State's sensitivity to them.

In the absence of any universally accepted definition of cybercrime, investigation of cross-border crime cases is carried on according to the procedural law of the place where the cybercrime is committed.

The problems arising due to divergence of laws and procedure of different nations may be eliminated to a considerable extent if at least major cybercrimes are uniformly recognised and incorporated by all the countries in their penal laws. This would ensure uniformity as regards identification of various actions as cybercrime.

Since these crimes have wide ranging ramifications, the penalties imposable on cyber offenders should be stringent and even exemplary so that they may desist from indulging in cyberspace criminality.

The question of a nation's jurisdiction in case of a cybercrime committed outside the country but having disastrous effect on that country itself, still remains unresolved as there is no general consciousness of different nations on this vital issue. The jurisdictional uncertainty regarding crimes committed in cyberspace has made committing of such crime easier but punishing the perpetrator thereof more difficult.

Therefore, the need of the hour is drafting of a uniform global cyber law with the co-operation of all the countries of the world. Jurisdictional uncertainty as regards the investigation and trial of cybercrime is perhaps the most ticklish problem which the law enforcement agencies all over the world are facing.

Cyber criminals may cause irreparable damage to victim(s) from a distant place without the risk of being spotted out or identified. This enables them to commit crimes beyond national borders without being physically present at the scene of crime.

The cross-country jurisdictional nature of internet and lack of adequate international co-operation to address the problem of cross-border cyber criminality enables criminals to escape arrest and prosecution. Therefore, in order to meet the jurisdictional challenges involved in cybercrimes, it has been suggested that an International Criminal Tribunal[9] with global jurisdiction be set up with power to investigate, try and punish cybercrime criminals.

15. Global Code of Digital Law for resolving IPR related Disputes:

[9] As suggested by G-8 contries in the Paris Convention on cyber crimes held in France in May, 2000.

It has been generally accepted that intellectual property is going to be the real estate of the Third Millennium[10].The information technology revolution during the closing years of twentieth century has opened scope for new variety of disputes in IPR regime, both at national and international level.

The resolution of these disputes needs a global Code of Digital Law to be developed which should have universal acceptance all over the world. This is all the more necessary in view of the expanding dimensions of IPR transactions having multi-national ramifications.

16. The menace of cyber terrorism:

Perhaps, the greatest threat posed by computer system and internet is that of cyber terrorism. It has changed the traditional concept of terrorism as the development of information technology has enabled terrorists to acquire more sophisticated and destructive technology and weapons to attack their targets[11].

The damage caused by the cyber terrorists is so catastrophic and irreparable that it completely shatters the National security and adversely affects the nation's economy. Presently, cyber terrorism has assumed international dimensions therefore, there is need to tackle this problem by developing e-security technology and adopting stringent penal policy both at the national as well as international level.

It may be suggested that India should make use of SAARC[12] forum to evolve consensus among the member countries about the need for concerted efforts to curb cyber criminality particularly cyber terrorism through regional co-operation. Efforts should also be made to acquire advance cyber technology from the developed countries adopting a mutual Code of Cyber Legislation.

17. Special Cyber Crime Investigation Cell for Hi-tech crimes:

In keeping with the demand of time, the setting up of a Cybercrime Investigation Cell under the Central Bureau of Investigation (CBI) was notified in September, 1999 which actually started functioning with effect from March 31, 2000.

The cell is headed by a Superintendent of Police and has jurisdiction all over India. It has the power to investigate the offences specified in Chapter XI of the Information Technology Act, 2000 and is also empowered to probe into other hi-tech crimes. There are presently six cybercrime investigation cells functioning in India with headquarters in Delhi, Mumbai, Chennai, Bangalore, Hyderabad and Kolkata.

Similar to the establishment of Special Cyber Crime Investigation Cell of CBI, there has been a growing demand for setting up Cyber Crime Police Stations by the State Governments. Taking initiative in this

[10] Choubey R.C. : An Introduction to Cyber Crime and Cyber Law, 2008 p. 778.
[11] Terrorist attack on U.S. World Trade Center (WTC) on 11 September, 2001 and on Indian Parliament on 13 December, 2001; Taj and Oberai Hotel, Mumbai on 26 November, 2008 etc. are the glaring examples of blatant misuse of computer technology for heinous cybercrimes.
[12] South Asian Association for Regional Co-oporation.

direction, the State of Karnataka was the first to set up the country's first Cyber Crime Police Station on August 30, 2001, which has jurisdiction all over the State. Subsequently, Cyber Police Cells were also set up in the metropolitan cities for handling cybercrimes. These cells are manned by specially qualified and trained police officials assisted by computer experts as and when required for the investigation of cyber crimes. But most States have no special police cyber cells and the cybercrimes are being handled by the general police. It is therefore, suggested that it should be mandatory for each State to set up at least one Special Cyber Crime Police Station well equipped with electronic technology and computer trained staff where complaints relating to cybercrime could be launched online so that hi-tech cybercrimes could be investigated efficiently and expeditiously. The police official working in these special cells should be empowered to conduct search of publicly accessible data or data in private systems, computer equipments, disk etc. with the prior permission by the concerned magistrate.

18. e-Judiciary and Video-conferencing for speedy justice:

In order to evolve right standards and practices in the emerging area of cyberspace crime adjudication, the three phased e-judiciary framework as proposed under the National Policy on Information and Communication Technology (NICT) must be completed within the prescribed time limit latest by the year ending 2010, so as to ensure speedy disposal cybercrime cases.

The national e-Court project started in July, 2007 for the creation of e-judiciary and e-governance grid covering India's entire judicial system would certainly ensure transparency, speed and fairness in the adjudication of cybercrime cases. It would reduce work-load of the courts and ensure speedy disposal of cases as also eliminate problems associated with paper-based records such as their collection, maintenance, retention etc. It is much easier to retain and retrieve electronic record.

The courts in India, have already adopted the system of videoconferencing for recording evidence of witnesses or under trial prisoners etc. at the district level, which has reduced the security risk of the prisoners escaping during transportation and has helped in saving the valuable time of the courts. Further expansion of the video-conferencing in subordinate courts needs to be accelerated.

It hardly needs to be stressed that computerization can help in enhancing the productivity of judicial work. It can create accessible database to help Judges, lawyers and litigants etc. as also facilitate case-management by the courts. It would certainly be a holistic approach to judicial reforms which encompass a wide variety of multifaceted issues such as up gradation of skill, quality improvement, adoption of ADR mechanism, revamping infrastructural gadgets and so on.

19. Need For Cyber Crime Reporter or Cyber Law Journal:

So far computer crime statistics are concerned; they do not reflect the true picture of incidence of cybercrimes. The reason being that operational speed and capacity of computer software, both makes it very difficult to detect cybercrime.

That apart, many victims of computer crime desist from reporting the crime because they apprehend unnecessary harassment and waste of time, energy and money in litigation which may drag on for years. The trading community and businessmen are particularly reluctant to report having fallen a victim to cybercrime due to the fear of adverse publicity, like loss of goodwill, embarrassment or harmful repercussions.

The lack of necessary technological expertise to deal with cybercrime on the part of law enforcement agencies is also a contributing factor for non-reporting of cybercrime cases by the victim(s). The intangible nature of cybercrime and anonymity of the perpetrator of the crime further complicates the issue of cybercrime reporting.

In short, it may be concluded that reporting of cybercrime cases is, by and large, scanty and whatever cases are reported, they are mostly either dropped for want of sufficient evidence or withdrawn or compromised by the parties-before they are finally disposed of by the court.

However, in view of the consistently rising graph of the incidence of cybercrimes and more and more cases coming before the courts for adjudication, it would be worthwhile to start publication of a 'Cyber-Crime Reporter' or 'Cyber Law Journal' for the benefit of the members of the Bar Bench, police and enforcement agencies and all others who are concerned with the detection, investigation and prosecution of cybercrime and criminals.

20. Digital Time Stamping System (DTS):

The Information Technology Act, 2000, allows transactions signed electronically to be recognised and made enforceable by law but there is no mechanism or device to know as to when and exactly at what time the particular electronic document was prepared and signed electronically.

The non-availability of any reliable evidence to establish the exact date and time when the disputed electronic document was made and signed leaves enough margin for uncertainty resulting in weakening of the prosecution case in such cybercrimes. This problem can be overcome by introducing a electronic device called 'Digital Time Stamping System' (DTS) in electronic transactions.

It consists of an apparatus called 'Tamperproof Box', in which a highly secured time-stamping server is used to create digital time stamps (DTS). The system has been successfully working in the United States for the last so many years.

21. Need for Universalisation of Cyber Law:

It has been generally observed that the perpetrators of cyber crime usually exploit the weaknesses inherent in the computer which is being used or attacked. Therefore, some special security measures may be adopted to prevent unauthorised use of the computer systems.

It is often alleged that the domestic laws controlling computer security are mostly directed to safeguard national safety, security and integrity rather than providing adequate protection to computer users, whether they are individuals or corporate entities. Therefore, the criminal laws of various countries including cyber law should be universalised so as to extend adequate protection to citizens, institutions, organisations, government and non-government agencies and society as a whole against the menace of cyber crime.

In the Indian setting, there is need to inculcate information consciousness among the Indian citizens. Though the Information Technology Act, 2000 as amended in 2008, has reasonably succeeded in providing relief to computer owners/users by extending the reach of law to almost all the online criminal activities and increasing awareness among the people, but it is not a foolproof law as yet since it was primarily enacted for the promotion of e-commerce to meet the needs of globalisation and liberalisation of economy.

The Act still suffers from certain lacunae as it does not provide adequate security against web-transactions nor does it contain adequate provisions to prevent securities fraud, stock confidentiality in the internet trading although the Securities Exchange Board of India (SEBI) has notified that trading of securities on internet is legally recognised and valid.

The comprehensive legislation brought out in the form of Information Technology (Amendment) Act, 2008 will certainly enable cracking down on crimes against information technology and cyber frauds which are often committed by the business processing outsourcing (BPO) agencies operating in the country.

It will also help in preventing data theft by call center employees. The amendment Act has provided a legal framework for crimes like video-voyeurism, e-commerce frauds, fraudulent impersonation called ‘phishing’, identity theft etc.

The Indian information technology law recognises the extra-territorial jurisdiction of cyber law but it cannot be effectively implemented in cases where the culprit (mostly the hacker) happens to be in a country with which India has no extradition treaty.

This problem may be resolved by making a suitable amendment in the law that cyber criminals from non-extradition countries can be brought to India for trial and prosecution in accordance with the established principles of international law.

Finally, it may be concluded that in the present computer age of 21st century, internet has influenced every facet of human life and no one can even think of life without the use of computers.

Therefore, in the present scenario, it is highly desirable that the computer technology should be preserved for the progress and prosperity of the society rather than being allowed to be misused by the criminal conduits for perpetration of crimes. At present, there are number of websites in the cyberspace that provide powerful tools for communicating, storing and processing information.

The web service providers should therefore, exercise due diligence and caution while pasting information in their web page. The ease with which the data and information flows through the internet across the world may sometimes be exploited by the criminals for the commission of crimes, which may be a serious cause of concern for the law-enforcement agencies at the national as well as the international level.

Bibliography:

Articles:

1. Walter. B. Wriston, The Twilight of Sovereignty : How the Information Technology Revolution is Transforming Our World (2003) p.31
2. John Naugent,Texas Woman,s University,DOI:10.4018/9781591409915.ch004
3. Cyber Terrorism, By Kevin coleman, Technolytics, october 10, 2003 http://www.symante.com/avcerter/reference/cyberterrorism.pdf.
4. Choubey R.C.;An Introduction to Cyber Crime and Cyber Law, 2008 p. 778.

Convention

1. Section 1, Chapter II of the European Convention document which contains Articles 2 to 13 defining ten cybercrimes under five separate titles,
2. As suggested by G-8 countries in the Paris Convention on cyber crimes held in France in May, 2000.

Bare Act:

1. The Information Technology Act, 2000 which came into force w.e.f. October 17, 2000.

Books

1. Cyber crimes, Electronic evidence & investigation legal issues, Nabhi Publication
2. An introduction to cyber law, Central Law Publication
3. Cyber Law in India, Pioneer Books
4. Cyber Law Simplified, TATA McGraw Hill
5. Law relating to Computers, Internet & E-commerce, Universal Law Publishing Co. Pvt. Ltd.
6. Cyber Laws, Universal Law Publishing Co.
7. Information Technology Law & Practice, Universal Lexis Nexis
8. Cyber crime & Terrorism, Swastik Publications

Case Study

1. Taj and Oberai Hotel, Mumbai on 26 November, 2008
2. Terrorist attack on U.S. World Trade Center (WTC) on 11 September, 2001
3. Indian Parliament on 13 December, 2001