CYBER LAW AND INFORMATION TECHNOLOGY

R. M. Kamble *

Abstract: Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done. The misuse of the technology has created the need of the enactment and implementation of the cyber laws. Today, computers play a major role in almost every crime that is committed. Citizens should not be under the impression that cyber crime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminals intentions encouraged by the so-called anonymity that internet provides. The Paper focuses on new legislation which can cover all the aspects of the Cyber Crimes should be passed so the grey areas of the law can be removed.

Keywords: Cyber Law, Information Technology, Cyber Crime, Computer, Enforcement, Data storage, Internet.

Introduction:

In any field of human activity Success leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe.

Recently, many information technology (IT) professionals lacked awareness of an interest in the cyber crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cyber crime: **law enforcement agencies** and **computer professionals.** Yet close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe "place" for its users.

Information is a resource which has no value until it is extracted, processed and utilized. Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done.

Information technology is affecting us as individual and as a society. Information technology stands firmly on hardware and software of a computer and tele-communication infrastructure. But this is only one facet of the information Technology, today the other facets are the challenges for the whole world like cyber crimes and more over cyber terrorism. When Internet was first developed, the founding fathers hardly had any inkling that internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level.

The misuse of the technology has created the need of the enactment and implementation of the cyber laws. As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. According to Donn Parker , "For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs." but whether this cyber laws are capable to control

* Teaching Assistant, Karnatak University's Sir Siddappa Kambali Law College, Karnatak University, Dharwad

the cyber crime activities, the question requires the at most attention.

Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cyber crime: **law enforcement agencies** and **computer professionals.** Yet close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe "place" for its users.

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cyber criminal. IT professionals need good definitions of cyber crime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cyber crimes is to sort all the acts that can be considered cyber crimes into organized categories.

What is a Computer Crime?

a. Criminals Can Operate Anonymously Over the Computer Networks.
b. Hackers Invade Privacy.
c. Hackers Destroy "Property" in the Form of Computer Files or Records.
d. Hackers Injure Other Computer Users by Destroying Information Systems.
e. Computer Pirates Steal Intellectual Property.

Definition of Cyber Crime

Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both".

In generally the term cybercrime was analyzed into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.
There are more concrete examples, including
i. Unauthorized access
ii. Damage to computer data or programs
iii. Computer sabotage
iv. Unauthorized interception of communications
v. Computer espionage

These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and agreement—for determining just what we mean by the term ***cybercrime.***

Classification of Cyber Crimes: *The Information Technology Act deals with the following cyber crimes along with others:*
o Tampering with computer source documents
o Hacking
o Publishing of information, which is obscene in electronic form
o Child Pornography
o Accessing protected system
o Breach of confidentiality and privacy

Cyber crimes other than those mentioned under the IT Act

o Cyber Stalking
o Cyber squatting
o Data Diddling
o Cyber Defamation

o Trojan Attack
o Forgery
o Financial crimes
o Internet time theft
o Virus/worm attack
o E-mail spoofing
o Email bombing
o Salami attack
o Web Jacking

Cyber law and Terrorism

Cyber crime and cyber terrorism are both crimes of the cyber world. The difference between the two however is with regard to the motive and the intention of the perpetrator.

While a cyber crime can be described simply as an unlawful act wherein the computer is either a tool or a target or both, cyber terrorism deserves a more detailed definition. One can define cyber terrorism as a premeditated use of disruptive activities or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives..

Cyber offenders:

Any person who commits an illegal act with a guilty intention or commits a crime is called an offender or a criminal. In this context, any person who commits a Cyber Crime is known as a Cyber Criminal. The Cyber Criminals may be children and adolescents aged b/w 6-18 years, they may be organized hackers, may be professional hackers or crackers, discontented employees, cheaters or even psychic persons.

a. Kids & Teenagers (age group 9-16 etc.): This is really difficult to believe but it is true. Most amateur hackers and cyber criminals are teenagers. To them, who have just begun to understand what appears to be a lot about computers, it is a matter of pride to have hacked into a computer system or a website. There is also that little issue of appearing really smart among friends. These young rebels may also commit cyber crimes without really knowing that they are doing anything wrong.

According to the BBC , Teen hackers have gone from simply trying to make a name for them selves to actually working their way into a life of crime from the computer angle. According to Kevin Hogan , One of the biggest changes of 2004 was the waning influence of the boy hackers keen to make a name by writing a fast-spreading virus. Although teenage virus writers will still play around with malicious code, 2004 saw a significant rise in criminal use of malicious programs. The financial incentives were driving criminal use of technology.

Another reason for the increase in number of teenage offenders in cyber crimes are that many of the offenders who are mainly young college students are unaware of its seriousness. Recently the Chennai city police have arrested an engineering college student from Tamil Nadu for sending unsolicited message to a chartered accountant. The boy is now released on bail. So counseling session for college students has to be launched to educate them on the gravity and consequences emanating from such crimes.

In September, 2005, A Massachusetts teenager pleaded guilty in federal court in Boston for a string of hacking crimes reported to include the February compromise of online information broker Lexis Nexis and socialite Paris Hilton's T-Mobile cellular phone account. The US Court noted that the number of teenage hackers is on the rise and only the lowest 1 percent of hackers is caught.

In the above instance, the judge imposed a sentence of 11 months' detention in a juvenile facility. If he had been an adult, he would have faced charges of three counts of making bomb threats against a person or property, three counts of causing damage to a protected computer system, two counts of wire fraud, one count of aggravated identity theft and one count of obtaining information from a protected computer in furtherance of a criminal act. This is clearly a deviation from the traditional principles of criminal law.

b. Organized hacktivists : Hacktivists are hackers with a particular (mostly political) motive. In other cases this reason can be social activism, religious activism, etc. The attacks on approximately 200 prominent Indian websites by a group of hackers known as Pakistani Cyber Warriors are a good example of political hacktivists at work.

c. Disgruntled employees: One can hardly believe how spiteful displeased employees can become. Till now they had the option of going on strike against their bosses. Now, with the increase independence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes, which can bring entire systems down.

d. Professional hackers (Corporate espionage): Extensive computerization has resulted in business organizations storing all their information in electronic form. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. The temptation to use professional hackers for industrial espionage also stems from the fact that physical presence required to gain access to important documents is rendered needless if hacking can retrieve those.

Criminal Law – General Principles

According to criminal law, certain persons are excluded from criminal liability for their actions, if at the relevant time; they had not reached an age of criminal responsibility. After reaching the initial age, there may be levels of responsibility dictated by age and the type of offense allegedly committed.

Governments enact laws to label certain types of activity as wrongful or illegal. Behavior of a more antisocial nature can be stigmatized in a more positive way to show society's disapproval through the use of the word criminal. In this context, laws tend to use the phrase, "age of criminal responsibility" in two different ways:
1. As a definition of the process for dealing with alleged offenders, the range of ages specifies the exemption of a child from the adult system of prosecution and punishment. Most states develop special juvenile justice systems in parallel to the adult criminal justice system. Children are diverted into this system when they have committed what would have been an offense in an adult.

2. As the physical capacity of a child to commit a crime. Hence, children are deemed incapable of committing some sexual or other acts requiring abilities of a more mature quality.

The age of majority is the threshold of adulthood as it is conceptualized in law. It is the chronological moment when children legally assume majority control over their persons and their actions and decisions, thereby terminating the legal control and legal responsibilities of their parents over and for them. But in the cyber world it is not possible to follow these traditional principles of criminal law to fix liability. Statistics reveal that in the cyber world, most of the offenders are those who are under the age of majority. Therefore, some other mechanism has to be evolved to deal with cyber criminals.

Ethics and morality in different circumstances connotes varied and complex meanings. Each and everything which is opposed to public policy, against public welfare and which may disturb public tranquility may be termed to be immoral and unethical. In the past terms such as imperialism, colonialism, apartheid, which were burning issues have given way to cyber crime, hacking, 'cyber-ethics' etc.

Positive Aspects of the IT Act, 2000:

1. Prior to the enactment of the IT Act, 2000 even an e-mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the IT Act, 2000 changed this scenario by legal recognition of the electronic format. Indeed, the IT Act, 2000 is a step forward.

2. From the perspective of the corporate sector, companies shall be able to carry out electronic commerce using the legal infrastructure provided by the IT Act, 2000. Till the coming into effect of the Indian Cyber law, the growth of electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the IT Act, 2000.

4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy if any one breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the IT Act, 2000 is in the form of monetary damages, by the way of compensation, not exceeding Rs. 1, 00, 00,000.

5. IT Act, 2000 has defined various cyber crimes which includes hacking and damage to the computer code. Prior to the coming into effect of the Indian Cyber law, the corporate were helpless as there was no legal redress for such issues. But the IT Act, 2000 changes the scene altogether.

The Grey Areas of the IT Act, 2000

1. The IT Act, 2000 is likely to cause a conflict of jurisdiction.

2. Electronic commerce is based on the system of domain names. The IT Act, 2000 does not even touch the issues relating to domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.

3. The IT Act, 2000 does not deal with any issues concerning the protection of Intellectual Property Rights I the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes.

4. As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The IT Act, 2000 does not cove various kinds of cyber crimes and Internet related crimes. These Include:-

a) Theft of Internet hours
b) Cyber theft
c) Cyber stalking
d) Cyber harassment
e) Cyber defamation
f) Cyber fraud
g) Misuse of credit card numbers
h) Chat room abuse

5. The IT Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.

6. Another grey area of the IT Act is that the same does not touch upon any anti- trust issues.

7. The most serious concern about the Indian Cyber law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers. It seems that the Parliament would be required to amend the IT Act, 2000 to remove the grey areas mentioned above.

Citizens should not be under the impression that cyber crime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminals intentions encouraged by the so-called anonymity that internet provides.

The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cyber crime. There have only been few cyber crime convictions in the whole country, which can be counted on fingers. We need to ensure that we have specialized procedures for prosecution of cyber crime cases so as to tackle them on a priority basis,. This is necessary so as to win the faith of the people in the ability of the system to tackle cyber crime. We must ensure that our system provides for stringent punishment of cyber crimes and cyber criminals so that the same acts as a deterrent for others.

Conclusion:

The new legislation which can cover all the aspects of the Cyber Crimes should be passed so the grey areas of the law can be removed. The recent blasts in Ahmedabad, Bangalore and Delhi reflects the threat to the mankind by the cyber space activities against this I personally believes that only the technology and its wide expansion can give strong fight to the problems. The software's are easily available for download should be restricted by the Government by appropriate actions. New amendment should be including to the IT Act, 2000 to make it efficient and active against the crimes. The training and public awareness programs should be organized in the Companies as well as in common sectors. The number of the cyber cops in India should be increased. The jurisdiction problem is there in the implementation part which should be removed because the cyber criminals does not have any jurisdiction limit then why do the laws have, after all they laws are there, to punish the criminal but present scenario gives them the chance to escape

Today in the present era there is a need to evolve a 'cyber-jurisprudence' based on which 'cyber-ethics' can be evaluated and criticized. Further there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline

The Information Technology Act 2000 was passed when the country was facing the problem of growing cyber crimes. Since the Internet is the medium for huge information and a large base of communications around the

world, it is necessary to take certain precautions while operating it. Therefore, in order to prevent cyber crime it is important to educate everyone and practice safe computing.

Following Frank William Abagnale & Robert Morris, many other hackers are intending to make use of their skills for better purposes. This trend continues even now where companies as their security analysts hire the brilliant hackers. Also, there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline. In the cyberspace, following traditional principles of criminal law to fix liability is not possible. Since most of the cyber criminals are those who are under the age of majority, some other legal framework has to be evolved to deal with them. Since cyber world has no boundaries, it is a Herculean task to frame laws to cover each and every aspect. But, however a balance has to be maintained and laws be evolved so as to keep a check on cyber crimes.

References:

1. Cyber Crimes and Real World Society by Lalitha Sridhar.
2. Cyber Law and Information Technology by Talwanth Singh Addl.Distt. And Sessions Judge, Delhi.
3. www.gahtan.com/cyberlaw - cyber law encyclopedia.
4. www.legalserviceindia.com/cyber-crimes.
5. www.indlii.org/Cyberlaw.aspx
6. www.cybercases.blogspot.com
7. Information Technology Act, 2000