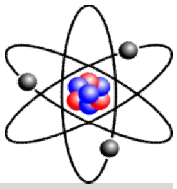
International Archive of Applied Sciences and Technology
Volume 3 [2] June 2012: 97 - 101
ISSN: 0976-4828

Website: www.soeagra.com/iaast/iaast.htm



Original Article

E-Governance Initiative in Cyber Law Making

Anil Kumar Gupta* and Manoj Kumar Gupta**
*Computer centre, Institute of Basic Science, Khandari Campus,Dr.B.R.A.University, Agra
**Daudyal vocational Institute, Khandari Campus, Dr.B.R.A.University,Agra

ABSTRACT
Nowadays most of financial and non-financial activities are done with computer and computer related services such as Internet. The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crime. The use of e- Governance the confidential document of government departments and organization is process and stored which can be hacked using computer. The IT Act provides the backbone for e-commerce and e-governance primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects.
Keywords: *e-Governance, Cyber Law, IT Act*

INTRODUCTION: WHAT IS CYBER LAW?

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.
Law includes the rules of conduct:

- That have been **approved** by the government, and
- Which are in **force** over a certain territory, and
- This must be obeyed by all persons on that territory.

Infringement of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.

Cyber law includes laws relating to:

- Cyber Crimes
- Electronic and Digital Signatures
- Intellectual Property
- Data Protection and Privacy

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The huge growth in electronic commerce (e-commerce) and online share trading has led to an unusual spurt in incidents of cyber crime.
Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures[1-4].
Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of **intellectual property** that relate to cyber space are covered by cyber law.
These include:

- **Copyright law** in relation to computer software, computer source code, websites, cell phone content etc,
- Software and source code **licences**
- **Trademark law** with relation to domain names, meta tags, mirroring, framing, linking etc
- **Semiconductor law** which relates to the protection of semiconductor integrated circuits design and layouts,
- **Patent law** in relation to computer hardware and software.

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc.

These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies [5-8].

NEED FOR CYBER LAW

There are various reasons why it is extremely difficult for conventional law to deal with cyberspace. Some of these are as follows:

- Cyberspace is an **intangible** dimension that is impossible to govern and regulate using conventional law.
- Cyberspace has complete **disrespect for jurisdictional boundaries.**
- Cyberspace handles **gigantic traffic volumes every second**. Millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
- Cyberspace is absolutely **open to participation by all**.
- Cyberspace offers never-seen-before **economic efficiency**. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.
- Electronic information has become the main object of cyber crime. It is characterized by **extreme mobility**, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.
- A software source code worth crores of rupees or a movie can be **pirated across the globe** within hours of their release [8-9].
- **Theft of** corporeal **information** (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions.

However, the problem begins when electronic records are copied quickly, unnoticeably and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner" and yet information gets stolen.

TECHNICAL ASPECTS

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

- **Unauthorized access & Hacking: -** Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer system or computer network. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer system network. Every act committed towards breaking into a computer or network is hacking. Hackers write or use readymade computer programs to attack the target computer. Some hackers hack for personal monetary gains. By hacking web server taking control on another person's website called as web hijacking.
- **Trojan Attack: -** The program that acts like something useful but do the things that are quiet damping. The programs of this king are called as Trojans. The name **Trojan Horse** is popular. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan.
- **Virus and Worm attack: -** A program that has capability to infect other programs and make copies of it and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms.
- **E- Mail & IRC related crimes:-**
    - ***Email spoofing:*** Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.
    - ***Email Spamming:*** Email "spamming" refers to sending email to thousands of users - similar to a chain letter. Sending malicious codes through email E- mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

- **Denial of Service attacks: -** Flooding a computer resource with more requests than it can handle. This cases the resource to crash thereby denying access of service to authorized users. Confidentiality it means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person. Such information should be protected [4,6,9].

CYBER LEGISLATIONS WORLDWIDE

To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore [10].

Countries with Cyber Updated Laws										
Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer Related Forgery	Computer Related Fraud
Australia	✔	✔	✔	✔		✔			✔	✔
Brazil		✔			✔	✔		✔		
Canada	✔	✔	✔	✔	✔	✔	✔			✔
Chile	✔	✔	✔	✔	✔					
China		✔		✔			✔			
Czech Rebublic		✔	✔		✔	✔				✔
Denmark		✔		✔						✔
Estonia		✔	✔	✔	✔	✔	✔	✔		✔
India		✔	✔	✔	✔	✔	✔	✔		✔
Japan	✔	✔	✔	✔	✔	✔		✔	✔	✔
Malaysia		✔				✔		✔		✔
Peru	✔	✔	✔	✔	✔	✔				✔
Philippines	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Poland		✔	✔	✔				✔		
Spain	✔	✔	✔					✔		✔
Turkey		✔	✔	✔	✔		✔	✔	✔	✔
United Kingdom		✔		✔	✔	✔		✔		
United States	✔	✔	✔	✔	✔	✔	✔	✔		✔

However, no country has fully resolved all the issues such as legal, enforcement and prevention of crime. The legislations enacted by different countries cover only few of the classified computers related offences. However, looking to the dynamic and fast changing technology, new types of offences may pop-up frequently.

Some of the major types of offences against which many countries across the globe have enacted various Acts are as follows: -

- Unlawful access to data in computers,
- Damaging data in computer etc.
- Possession of device to obtain unauthorised telephone facilities,
- Unauthorised access to computer and computer material

- Committing mischief with data.
- Data spying,
- Computer fraud,
- Forgery of prohibitive data,
- Alteration of data,
- Computer sabotage.
- False entry in an authentic deed
- False entry in permit licence or passport
- Electronic record made wrongfully
- Electronic record made wrongfully by public servant
- Interferences with business by destruction or damage of computer
- Interferences with computer
- Destruction of public document
- Destruction of private document
- Unauthorised access with intention to commit offences/ computer crimes
- Unauthorised use and interception of computer services
- Knowingly access of computer without authorisation related to national defence or foreign relation
- Intentional access of computer without authorisation to obtain financial information
- Unauthorised access of computer of a Govt. Deptt. Or agency
- Knowingly causing transmission of data/program to damage a computer network, data or program or withhold or deny use of computer, network etc.
- Knowingly causing transmission of data/program with risk that transmission will damage a computer network, data or program or withhold or deny use of computer, network etc, an unauthorised access of computer with intent to defraud.

ADVANTAGES OF CYBER LAWS

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much needed legal framework so that information is not denied legal effect. Validity or enforceability, Solely on the ground that it is in the form of electronic records. In view of the growth in transactions and communications carried out through electronic records. The Act seeks to empower government departments to accept filing. Creating and retention of official documents in the digital format. The Act had also proposed a legal framework for the authentication and origin of electronic records/ communications through digital signature. Firstly, the implications of these provisions for the e- businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. The Act now allows Government to issue notification on the web thus heralding with any office. Authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government. The IT Act also addresses the important issues of security to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date[7-10].

CONCLUSIONS

The conclusion may, therefore, be drawn that computer- related crime is a real, expanding phenomenon. Furthermore, a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers. The law of the Internet has already emerged, and we believe can continue to emerge with individual users voting to join the particular systems they find most congenial. However, this model also does not solve all problems. And various governance issues cannot be resolved overnight. We will need to redefine Cyber Legal processes in this new dynamic context. Finally, the Cyber Law defined as a thoughtful group conversation about

core values and distinct benefits to the Society will persist. But it will not, and should not be the same law as that applicable to physical, geographically defined territories.

RECOMMENDATIONS

The weak state of global legal protections against cyber crime suggests three kinds of action.

- **Firms should secure their networked information.**
  Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.
- **Governments should assure that their laws apply to cyber crimes.**
  National governments remain the dominant authority for regulating criminal behaviour in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat.
- **Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security.**
  To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cyber crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe (see www.coe.int), comprising 41 countries. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data.

Finally, it promotes cooperation among law enforcement officials across national borders.

REFERENCES

1. Blythe, Stephen E. (2007). China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce, Chicago-Kent Journal of Intellectual Property 7, 1.
2. Blythe, Stephen E. (2008). Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security, European Journal of Law and Economics 26:1, 75-103. Blythe, Stephen E., The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries, *Journal of Economics and Administrative Sciences* 22:1, 103.
3. Blythe, Stephen E. (May, 2008). Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security, Armenian Law Review;
4. K. C. and Traver, C. G., 2010, "e-commerce", ISBN#01361-00597, Prentice Hall, NJ
5. Cyber law : The Law of Internet by J. Rosenoer
6. Cyber Law & Its implication By J. Sruis
7. Cyber Law : Legal Principles of Emerging Technologies By Jeffrey A Helewitz
8. www. cyberlaws india. Net
9. www. madaan. com/ cyberlaw. html
10. www. cybersmart .in.