Research Paper Commerce

Cyber Laws and Cyber Crimes in India: A Critical Analysis

Dr. Kritika
ICSSR Post Doctoral Fellow, Department of Commerce, Maharshi Dayanand University, Rohtak

ABSTRACT

We all know and understand that the life around us is getting faster and competitive every passing day. With increasing work pressures and target deadlines everyone is really desperate to get someone help them in every aspect. And this help is offered by "Computers". The rationale behind taking this topic is very simple. India is the most happening IT destination in the world as on today. We are producing the best brains in the world. The best companies in the world hire Indians for their knowledge. Facts reveal that world's top ten companies have up to 10% Indians holding key posts in the company's executive body (board). World's best companies like Microsoft and Oracle have special cafes for Indian employees. And the knowledge and training provided here are far superior to many advanced countries. There are lakhs of student who graduate every year and learn about these new technologies and services.

KEYWORDS : Cyber Laws, Cyber Crimes, Information Technology Act

Computers have been one of the greatest inventions in the history of mankind; it has changed the whole world around us and shown as new and sophisticated techniques of doing the same old tedious jobs in a better fashion. Computer offered a plethora of services and human race started a never ending process of improving it. Right from the basic calculus devised by Mr. Charles Babbage till the latest and fastest multimillion dollar costing Super Computers, the improvisation is still on.

Internet made the world a smaller place. This technology was simply called as "Network of Networks". It means that when a smaller network of several computers is connected to a bigger network comprising of many such smaller network, it is called as internet.

The problem was serious, though the user can get share and transfer authentic data, some smart brains started looking for other data as well. This led to breach of privacy and security. Since the overall functioning of networking technologies remained the same it became really difficult to differentiate between a legitimate and a spoofed incoming connection. This led to another milestone development. Everybody felt a need of law that would be able to prevent the malpractices on the internet. And a new term was coined called **"Cyber Law".**

The scope and extent of cyber law was different with respect to geographical boundaries and usage of computer based technology. The nations which were better developed than others had a greater impact of computer and had better cyber laws as compared to others. With the introduction of cyber laws and better development in cryptographic techniques the internet technologies like E-Commerce. Electronic Commerce made it possible to make commercial transaction sitting at the comfort of the home or office. This involved financial data of the individual, banks, payment gateways and host of other servers. The computerization of other departments also made it an exciting field to explore the possibilities and exploit it.

The intentions were not evil in all the cases, most of the time it was curiosity and error finding techniques that led to the backdoors of certain computers or software programs. However it became a full fledged art of hacking and reverse engineering. Programmers started using various techniques to penetrated and peek into databases of government organizations and other institutions. Some of them started exploiting it regularly and understood the monetary benefits which were very lucrative. And thus a new type of crime came into existence called **"Cyber Crime".**

With advancement in technologies the problem started multiplying manifolds and cyber patrol troops were being developed to keep a check on this. Both the teams; Hack and Counter Hack; were trying their best to get other. The war is still on. Even today the dark worlds of underground do have a fleet of sophisticated highly intellectual computer nerds generally referred to as **"Hackers".**

Hackers are the bad guys who do all the wrong doing right from hacking into computers to software piracy to writing malicious automated codes to perform unsolicited things on a remote computer to reverse engineer source codes of the program etc. The list continues with illegal electronic fund transfers, email spoofing, spamming, pornography, denial of service attacks, man in the middle attacks, phishing attacks etc.

In present study the researcher has tried to find out the various types of crimes that are prevalent and various laws available in the Indian Legal System to curb them. The present study humble effort to evaluate the impact of cyber crimes across the globe with special reference to India.

Objectives of the Study

To make an Assessment of the Information Technology Act 2000

To give an insight in various types of crimes and the methodology used by criminals.

To create an awareness of Cyber Crimes among people

Importance of the Study

Importance of the topic can be judged on 3 primary issues. They are as follows:

Assessment of the Information Technology Act 2000-This is needed to understand the flaws and anomalies in the IT Act 2000. This will be helpful in improving our legal system and make an attempt to consider important issues if not covered under the jurisdiction of the act.

Understanding Cyber Crimes- This will give us an insight in various types of crimes and the methodology used by criminals. It will help to understand that which are considered as crime but people are unaware of it.

Protection against cyber attacks- This will help us in protecting ourselves from various types of cyber crimes and cyber attacks so that we can stay safe and protect ourselves.

It is quite evident that computers can either used as tool for attack or target for attack or both at the same time. Now with the inventions of better means of telecommunications and networking techniques even mobile phones come under the definition of a computer. Thus a PDA or a handheld device used to commit mischievous act is liable for the same punishment.

Even sending a pornographic picture or a vulgar SMS to anyone is a crime under IT Act 2000. But people are not aware of this or might be their attitude is casual. However when we underline the punishments and penalties associated with them, the gravity of the act is understood.

Thus with the above stated needs this project study is undertaken.

Research Methodology

The research methodology consists of collection of primary data and secondary data and their analysis. The secondary data consists of material collected form legal documents and GR's published by the government of India, books and magazines, while papers submitted by various authors on various topics.

NEED FOR CYBER LAW

The Etymology of the term "Cyber"

Although William Gibson is widely credited with coining the term "Cyberspace" in the 1980s, the prefix cyber is much older. The word is clipped off from the word cybernetics, which comes from the Greek "Kubernetes" meaning steersman or governor.

The English term "cybernetics" as we know it today was borrowed by the American Mathematician Norbert Wiener in the 1940s to mean the theory of control and communication processes. As computers became more popular, cybernetics became cyber as it was short and catchy. With the passage of time it was forgotten that the word is actually abbreviated from cybernetics. Hence, the term cyber tends to be used when speaking of computer or of computer networks from a broader perspective as opposed to the term virtual or digital.

With this reference to the meaning of the word cyber, cyber squatting, cyber terrorism and even cyber phobia become self explanatory.

Cyber Law

Cyber Law has often been defined as the "law governing cyberspace" or "Internet Law".

To define cyber law as the law governing cyberspace would perhaps spark off a debate regarding the correct definition of the term since the definition would be dependent upon how we construe the term cyberspace. A general reading of the term would suggest that cyberspace comes alive only when two or more computers are networked together.

If cyberspace refers to the Internet, then cyber law would be construed as law relating to the Internet, which would limit its scope. In such a case, which law would regulate electronic information stored a standalone computers?

On the other hand, if the term cyberspace is thought of as not being restricted to the Internet but a wider term that includes computers, computer networks, the Internet, data, software etc., then there would not be any problem in defining cyber law in the context of cyberspace.

Keeping in mind the etymology of the term cyber as discussed above, the term cyber law would mean law relating to computers and computer networks, encompassing all activities that take place in relation to information stored or exchanged using the same. This would not only encompass the Internet. (a vast network of smaller networks) but also standalone computers.

The need for cyber law (As a separate discipline)

The need for a separate body of law dealing with electronic information stored and communicated through computers has to be analyzed in the light of standalone computers as well as in the context of a network of computers, e.g., the Internet characterized by cyberspace.

Jurisprudential thought would probably hinge the development of cyber law on three factors. Firstly, the requirement for faster, efficient and reliable communication; secondly, the need for a paperless would and all the advantages that come with it; and thirdly, the increasing value of electronic information as a result of those needs.

As the increasing value of information stored in electronic form slowly assumes the form and characteristics of property, a legal regime is developing to protect this property.

Thus, electronic information (usually referred to as computer data) has become the main object of computer crime. It is characterized by an 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.

Above all, national solutions and restrictions for the free flow of information would be doomed to failure since the amount of data transferred in international computer networks makes control of their content neither possible nor socially desirable. Thus, international and supranational aspects of crime gain much more importance in cyberspace than in other comparable fields of crime.

All these facts make it extremely difficult for the existing models of legal regulation to cope with crime in cyberspace.

Scope of Information Technology Act 2000

Cyber law encompasses a wide variety of political and legal issues related to electronic commerce, electronic communication, the Internet and other communications technology, intellectual property, privacy, freedom of expression and jurisdiction.

Thus, Cyber Law encompasses laws relating to:

Electronic and Digital Signatures:

Electronic Signatures (especially Digital Signature) are fast becoming the de-facto standard for authentication of electronic records, Electronic Data Interchange, Emails etc.

Comprehensive laws are required so that uniform standards and procedures can be established. Thus laws relating to Electronic Signatures and law relating to digital signatures are a part of cyber law.

Computer Crimes:

Our growing dependence on computer and the Internet has made us all potential victims of Internet threats.

Some countries have enacted legislations that specifically deal with computer crime and yet others have adapted their existing laws to make computer crime an offence under existing statutes.

Intellectual Property:

Cyber law covers the intellectual property laws that relates to cyber space and its constituents.

This includes copyright law in relation to computer software, computer source codes etc; trademark law in relation to domain names; patent law in relation to computer software.

References

1. Information Technology Act 2000 (Bare Act). Published by Ministry of Law, Justice and Company Affairs.
2. Gazette of India on Blocking of websites. Published by Ministry of Communications and Information Technology.
3. Gazette of India: Extraordinary on Controller authority. Published by Ministry of Communications and Information Technology.
4. Gazette of India on Digital Signatures. Published by Ministry of Communications and Information Technology.