Cyber Laws: A Global Perspective

Manish Lunker
manishl@india.com

Introduction

In the today's era of rapid growth, Information technology is encompassing all walks of life all over the world. These technological developments have made the transition from paper to paperless transactions possible. We are now creating new standards of speed, efficiency, and accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used to store confidential data of political, social, economic or personal nature bringing immense benefit to the society.

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 enactment of necessary legislation in all countries for the prevention of computer related crime.

Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law-making and law-enforcing authorities find this new environment deeply threatening.

Why Cyber Laws At All

We may ask why is there a need for a separate law to govern the Cyber World?
This may also assume significance looking to the fact that the phenomenal spread of Internet has been enabled mainly due to the absence of a centralised regulating agency.
Anyone who has access to a computer and a telephone network is free to get hooked to the Internet. This uncontrollable growth of the Internet makes the need for regulation even more badly felt.

Systems across the globe have many different rules governing the behavior of users. These users in most of the countries are completely free to join/ leave any system whose rules they find comfortable/ not comfortable to them. This extra flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult for System Administrators to have a check on Frauds, Vandalism or Abuses, which may make the life of many online users miserable.

This situation is alarming as any element of distrust for Internet may lead to people avoiding doing transactions with online sites thereby directly affecting e-Commerce growth. The (Mis)Use of Internet as an excellent medium of communication may in some situations lead to direct damage to physical societies. Non-imposition of taxes on online transactions may have its destructive effect on the physical businesses and also government revenues. Terrorists may also make use of web to create conspiracies and make violence in the society.

Therefore, all of us whether we directly use Internet or not, will like to have some form of regulation or external control for monitoring online transactions and the cyber world for preventing any instability.

Cyber Crimes

"Computer or Cyber crimes are considered as illegal, unethical or unauthorised behaviour of people relating to the automatic processing and transmission of data, use of Computer Systems and Networks".

Common types of Cyber Crimes may be broadly classified in the following groups:-

1. Against Individuals: -
    a. Against Person: -

        i. Harassment through e-mails.
        ii. Cyber-stalking.
        iii. Dissemination of obscene material on the Internet.
        iv. Defamation.
        v. Hacking/cracking.
        vi. Indecent exposure.

    b. Against property of an individual: -

        i. Computer vandalism.
        ii. Transmitting virus.
        iii. Internet intrusion.
        iv. Unauthorised control over computer system.
        v. Hacking /cracking.

2. Against Organisations: -
    a. Against Government, Private Firm, Company, Group of Individuals: -

        i. Hacking & Cracking.
        ii. Possession of unauthorised information.
        iii. Cyber terrorism against the government organisation.
        iv. Distribution of pirated software etc.

3. Against Society at large: -

    i. Pornography (specially child pornography).
    ii. Polluting the youth through indecent exposure.
    iii. Trafficking.

Basic approaches for creation of Cyber Laws

Following are the basic approaches for creation of Cyber Laws, which will ensure the smooth governance of Internet globally:

a) Formulation of new laws and amendment of existing laws by nations within their present territorial boundaries thereby attempting to regulate all actions on the Internet that have any impact on their own population.

b) Nations may enter into multi-lateral international agreements to establish new and uniform rules specifically applicable to conduct on the Internet.

c) Creation of an entirely new international organisation, which can establish new rules and new means of enforcing those rules.

d) Guidelines and rules may naturally emerge from individual decisions like domain name and IP address registrations and by websites and users deciding about whom will they patronise.

All of these approaches have their own merits and demerits and we shall not go into those details here.

Establishing a Suitable framework

There is a dire need for the emergence of a well-defined framework of Cyber Laws, which should be able to do the following:

1) Create and implement a minimum set of guiding rules of conduct that would facilitate efficient Communications and reliable Commerce through the use of Electronic medium.

2) Define, punish and prevent wrongful actions that attack the electronic medium or harm others.

One of the greatest concerns of the field of Cyber Laws has been the absence (or rather delay) of a well-defined and comprehensive framework of law across the globe. Today's *Internet* was born in the early 1960's while the initial efforts for its regulation could only surface in the late 1990's. This problem has been further aggravated by the steep rise in usage of Internet in the recent years all over the world and that too in the absence of any appropriate legal framework.

Surely, the Cyber Law scenario is globally more complicated than traditional laws owing to the reason that the range of activities which are to be governed by these laws are largely technology driven, an area which is dynamically changing and is beyond anyone's control. However enactment of these laws pose opportunities for nations to carve model Cyber Societies for the future thereby taking a lead in becoming Global IT Powers.

Effective Implementation of any law is as critical an exercise as its enactment. A law implementing agency has to focus on the following major areas to be effective:

1. Creating a suitable climate thereby Inducing Self Compliance by the Society.
2. Regular monitoring of the scenario for reliable feedback.
3. Offering Openness and Flexibility to accept and incorporate necessary modifications at appropriate times.
4. Distinctly establishing the Authority-Responsibility guidelines for the Implementing Agency.

In order to be effective, it has to be ensured that the Law is Simple, fair and full of clarity. Failing this, the law may be misused to harass individuals resulting in its defiance. The implementing agency will then be compelled to take corrective actions to ensure implementation. This whole process may result in spread of corruption and polluting of the overall sentiments in society making the job of law implementing agencies more difficult.

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.

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 computer-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 (mostly at preliminary levels) are as follows: -

1. Unlawful access to data in computers,
2. Damaging data in computer etc.
3. Possession of device to obtain unauthorised telephone facilities,
4. Unauthorised access to computer and computer material
5. Committing mischief with data.
6. Data spying,
7. Computer fraud,
8. Forgery of prohibitive data,
9. Alteration of data,
10. Computer sabotage.
11. False entry in an authentic deed
12. False entry in permit licence or passport
13. Electronic record made wrongfully
14. Electronic record made wrongfully by public servant
15. Interferences with business by destruction or damage of computer
16. Interferences with computer
17. Destruction of public document
18. Destruction of private document
19. Unauthorised access with intention to commit offences/ computer crimes
20. Unauthorised use and interception of computer services
21. Knowingly access of computer without authorisation related to national defence or foreign relation
22. Intentional access of computer without authorisation to obtain financial information
23. Unauthorised access of computer of a Govt. Deptt. Or agency
24. Knowingly causing transmission of data/program to damage a computer network, data or program or withhold or deny use of computer, network etc.
25. 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.

Cyber laws in India

Keeping in line with other countries, India also has passed its first cyber law, The Information Technology Act 2000, which aims to provide the legal backbone for enabling e-commerce in the country. However the arrival of Internet resulted in the rise of new and complex legal issues.

Though India has a detailed and well-defined legal system in place, with laws like the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on. But at the time of enactment of these laws nobody could really visualise about the Internet. We must remember that all the existing laws in place in India were enacted keeping in mind the relevant political, social, economic, and cultural scenario of the corresponding time. As like the rest of the world, the existing laws of India also could not handle the various cyber space activities. As such the need arose for a Cyber Law.

Conclusions

The conclusion may, therefore, be drawn that computer-related crime is a real, (at least in respect of certain offences) expanding phenomenon. Furthermore, a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers.

Let's now once again review the alternatives available for establishing a comprehensive legal framework. Can we make only territorial laws applicable to online activities that have no relevant or perhaps even determinable geographic location? It seems to be very difficult. We must also allow responsible participants on the Internet to set their own rules and to help all concerned (online and offline). 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, could not, and should not be the same law as that applicable to physical, geographically defined territories.