Introduction to

Indian Cyber Law

This document is an extract from the book *IPR & Cyberspace – Indian Perspective* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws

www.asianlaws.org

1. Jurisprudence of Cyber Law

Jurisprudence studies the concepts of law and the effect of social norms and regulations on the development of law.

Jurisprudence refers to two different things.

1. The philosophy of law, or legal theory
2. Case Law

Legal theory does not study the characteristics of law in a particular country (e.g. India or Canada) but studies law in general i.e. those attributes common to all legal systems.

Legal theory studies questions such as:

1. What is law and legal system?
2. What is the relationship between law and power?
3. What is the relationship between law and justice or morality?
4. Does every society have a legal system?
5. How should we understand concepts like legal rights and legal obligations or duties?
6. What is the proper function of law?
7. What sort of acts should be subject to punishment, and what sort of punishments should be permitted?
8. What is justice?
9. What rights do we have?
10. Is there a duty to obey the law?
11. What value does the rule of law have?

Case law is the law that is established through the decisions of the courts and other officials.

Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the Courts helps clarify the real objectives and meaning of such laws.

This chapter first discusses the meaning of cyber law and the need for the separate discipline of cyber law.

This chapter covers the following topics:

1. What Is Cyber Law?
2. Need for Cyber Law
3. Jurisprudence of Indian Cyber Law
4. Evolution of Key Terms and Concepts
5. Evolution of Cyber Crime

1.1 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 (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Law encompasses the rules of conduct:

1. that have been **approved** by the government, and
2. which are in **force** over a certain territory, and
3. which must be **obeyed** by all persons on that territory.

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

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime. These crimes are discussed in detail further in this chapter. A comprehensive discussion on the Indian law relating to cyber crimes and digital evidence is provided in the **ASCL publication** titled "**Cyber Crimes & Digital Evidence – Indian Perspective**".

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. These issues are discussed in detail in the **ASCL publication** titled "**Ecommerce – Legal Issues**".

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.

These issues are discussed in detail in the **ASCL publication** titled "**IPR & Cyberspace - the Indian Perspective**".

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.

1.2 Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1. Cyberspace is an **intangible** dimension that is impossible to govern and regulate using conventional law.

2. Cyberspace has complete **disrespect for jurisdictional boundaries**. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

3. Cyberspace handles **gigantic traffic volumes every second**. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4. Cyberspace is absolutely **open to participation by all**. A ten-year-old in Bhutan can have a live chat session with an eight-year-old in Bali without any regard for the distance or the anonymity between them.

5. Cyberspace offers **enormous potential for anonymity** to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

6. 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.

7. 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.

8. A software source code worth crores of rupees or a movie can be **pirated across the globe** within hours of their release.

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, inconspicuously and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner" and yet information gets stolen.