

BCA- 602
CYBER LAW & INTERNET SECURITY

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.

The philosophy of law, or legal theory

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

What is law and legal system?

What is the relationship between law and power?

What is the relationship between law and justice or morality?

Does every society have a legal system?

How should we understand concepts like legal rights and legal obligations or duties?

What is the proper function of law?

What sort of acts should be subject to punishment, and what sort of punishments should be permitted?

What is justice?

What rights do we have?

Is there a duty to obey the law?

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.

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.

What is Cyber Law?

Law encompasses the rules of conduct:

that have been **approved** by the government, and which are in **force** over a certain territory, and 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:

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 enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal 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.

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.

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.

Need for Cyber Law

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.

Need for Cyber Law

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.

Need for Cyber Law

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.

Need for Cyber Law

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.

Jurisprudence of Indian Cyber Law

The primary source of cyber law in India is the **Information Technology Act, 2000 (IT Act)** which came into force on 17 October 2000.

The primary purpose of the Act is to provide **legal recognition to electronic commerce** and to facilitate filing of **electronic records with the Government**.

The IT Act also penalizes various **cyber crimes** and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore).

Jurisprudence of Indian Cyber Law

An **Executive Order** dated 12 September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate.

Minor errors in the Act were rectified by the **Information Technology (Removal of Difficulties) Order, 2002** which was passed on 19 September 2002.

Jurisprudence of Indian Cyber Law

The IT Act was amended by the **Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002**. This introduced the concept of electronic cheques and truncated cheques.

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government.

It also provides for payment and receipt of fees in relation to the Government bodies.

On the same day, the **Information Technology (Certifying Authorities) Rules, 2000** also came into force.

These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA.

These rules were amended in 2003, 2004 and 2006.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA.

Two important guidelines relating to CAs were issued. The first are the **Guidelines** for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001.

Next were the **Guidelines** for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002.

The **Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000** also came into force on 17th October 2000.

These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.

The **Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003** prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.

On 17th March 2003, the **Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003** were passed.

These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc.

These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the **public interest litigation filed by students of Asian School of Cyber Laws (ASCL)**.

The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers.

The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice

A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this the Central Government passed an order dated 23rd March 2003 appointing the "Secretary of Department of Information Technology of each of the States or of Union Territories" of India as the adjudicating officers.

The **Information Technology (Security Procedure) Rules, 2004** came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records.

Also relevant are the **Information Technology (Other Standards) Rules, 2003**.

An important **order relating to blocking of websites** was passed on 27th February, 2003.

Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

The **Indian Penal Code** (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital Evidence is to be collected and proven in court as per the provisions of the **Indian Evidence Act** (as amended by the IT Act).

In case of bank records, the provisions of the **Bankers' Book Evidence Act** (as amended by the IT Act) are relevant.

Investigation and adjudication of cyber crimes is done in accordance with the provisions of the **Code of Criminal Procedure** and the IT Act.

The Reserve Bank of India Act was also amended by the IT Act.

Evolution of key terms and concepts

To understand the jurisprudence of cyber law, it is essential to examine how the definitions of key terms and concepts have developed.

According to section 2(1)(i) of the IT Act

"computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

Simply put, a computer has the following characteristics:

It is a high-speed **data processing device** or system.

It may be **electronic, magnetic, optical** etc.

It performs **logical, arithmetic, and memory functions**

These functions are performed by manipulations of electronic, magnetic or optical impulses.

Computer includes

all input facilities,
all output facilities,
all processing facilities,
all storage facilities,
all computer software facilities, and
all communication facilities

which are connected or related to the computer in a computer system or network.

According to American law, **electronic** means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

[Title 15, Chapter 96, Sub-chapter I, section 7006(2), US Code].

Magnetic means having the properties of a magnet; i.e. of attracting iron or steel e.g. parts of a hard disk are covered with a thin coat of magnetic material.

Simply put, an **optical computer** uses light instead of electricity to manipulate, store and transmit data. Development of this technology is still in a nascent stage.

Optical data processing can perform several operations simultaneously (in parallel) much faster and easier than electronics.

Optical fibre is the medium and the technology associated with the transmission of information as light pulses along a glass or plastic wire or fibre.

Optical fibre carries much more information than conventional copper wire and is in general not subject to electromagnetic interference.

A **data processing device or system** is a mechanism that can perform pre-defined operations upon information.

The following are illustrations of **functions** in relation to a conventional desktop personal computer.

saving information on a hard disk,
logging on to the Internet,
retrieving stored information,
calculating mathematical formulae.

Logical functions, simply put, refer to non- arithmetic processing that arranges numbers or letters according to a predefined format e.g. arranging numbers in ascending order, arranging words alphabetically etc.

Arithmetic functions, simply put, are operations concerned or involved with mathematics and the addition, subtraction, multiplication and division of numbers.

Memory functions, simply put, refer to operations involving storage of data.

Input facilities are those which transfer information from the outside world into a computer system. E.g. keyboard, mouse, touch screen, joystick, microphone, scanner etc.

Output facilities are those which transfer data out of the computer in the form of text, images, sounds etc to a display screen, printer, storage device etc.

Hard disks, USB disks, floppies act as both input and output facilities.

Processing facilities primarily refers to the Central Processing Unit (CPU) of a computer. Referred to as the “brain” of the computer, the CPU processes instructions and data.

Storage facilities include hard disks and other data storage facilities. This term would also include the physical cabinet in which a computer is housed.

Computer software facilities refer to the operating system and application software that are essential for a computer to function in a useful manner.

Communication facilities include the network interface cards, modems and other devices that enable a computer to communicate with other computers.

Illustrations

Considering the wide definition given to the term computer by the IT Act the following are examples of “computers”:

desktop personal computers

mobile phones

microwave ovens

computer printers

scanners

installed computer software

Automatic Teller Machine (ATM)

“smart” homes which can be controlled through the Internet

Relevant Case Law

In an interesting case, the Karnataka High Court laid down that **ATMs are not computers, but are electronic devices under the Karnataka Sales Tax Act, 1957.**

Diebold Systems Pvt Ltd [a manufacturer and supplier of Automated Teller Machines (ATM)] had sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 on sale of ATMs.

Relevant Case Law

The majority view of the ARA was to classify ATMs as "**computer terminals**" liable for **4% basic tax** as they would fall under Entry 20(ii)(b) of Part 'C' of Second Schedule to the Karnataka Sales Tax Act.

The Chairman of the ARA dissented from the majority view. In his opinion, ATMs would fit into the description of **electronic goods**, parts and accessories thereof. They would thus attract **12% basic tax** and would fall under Entry 4 of Part 'E' of the Second Schedule to the KST Act.

Relevant Case Law

The Commissioner of Commercial Taxes was of the view that the ARA ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals.

The High Court of Karnataka acknowledged that **the IT Act provided an enlarged definition of "computers"**. However, the Court held that **such a wide definition could not be used for interpreting a taxation related law** such as the Karnataka Sales Tax Act, 1957.

Relevant Case Law

The High Court also said that an **ATM is not a computer by itself and it is connected to a computer** that performs the tasks requested by the persons using the ATM. The computer is connected electronically to many ATMs that may be located at some distance from the computer.

Relevant Case Law

Diebold Systems Pvt Ltd vs. Commissioner of Commercial Taxes ILR 2005 KAR 2210, [2006] 144 STC 59(Kar)

Data

According to section 2(1)(o) of the IT Act

“data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

Simply put, data is

a representation of information, knowledge, facts, concepts or instructions,

prepared or being prepared in a formalized manner,

processed, being processed or sought to be processed in a computer.

Illustration

Sanya is typing a document on her computer. The moment she presses keys on her keyboard, the corresponding alphabets are shown on her screen. But in the background some parts of the document are stored in the RAM of her computer (*being processed*) while other parts are stored on the hard disk (*processed*). At any given instant some information would be passing from her keyboard to the computer (*sought to be processed*).

Data can be in many forms such as

computer printouts,

magnetic storage media e.g. hard disks,

optical storage media e.g. CD ROMs, DVDs, VCDs

punched cards or tapes i.e. a paper card in which holes are punched.

Illustration

The electronic version of any book stored on your computer or on a CD would be “data”. A printout of the electronic version of this book will also be “data”.

Computer Software

Computer **software** is a general term that describes a collection of:

computer programs,
procedures and
documentation.

Computer **hardware**, on the other hand, consists of the physical devices that can store and execute computer software.

Illustration

Sanya downloads the OpenOffice software from the Internet. In effect what she downloads is an **executable** file. She double-clicks on the executable file and begins to **install** the software on her computer.

During the installation she specifies the part (drive and folder name etc) of the hard disk where the software files must be saved.

During the installation the software also makes entries in system files (e.g. registry) maintained by the operating system (e.g. Windows XP).

Once the installation is complete, Sanya can **run the software**. When she runs the software, relevant software files get loaded into **RAM** and are subsequently executed in the **CPU** (central processing unit).

Computer software can be divided into two fundamental categories – **system software** and **application software**.

Application software uses the computer directly for performing user tasks. System software enables the application software to use the computer's capabilities.

Analogy

An oil company drills for oil on the sea bed. This oil is then processed and provided to the customer in the form of petrol for his car. Here the petrol is like the application software – it helps the user to run his car. The oil company is like the system software

– it enables the petrol to be taken to the user.

System software can be of various types such as

operating systems which form the platform for all other software on a computer.

device drivers which allow computer programs to interact with a hardware devices such as printers, scanners etc,

programming tools which help programmers to develop and test other programs.

compilers which compile the source code into the object code,

linkers which link object code files (and libraries) to generate an executable file.

utility software that helps manage and tune the computer hardware, operating system or application software.

Application software include

1. word processors (e.g. Microsoft Word),
2. spreadsheets (e.g. Microsoft Excel)
3. presentation software (e.g. Microsoft Powerpoint)
4. media players (e.g. Microsoft Windows Media Player)
5. games (e.g. Need for Speed, Age of Empires)
6. forensic software (e.g. Winhex, X-Ways Forensics)
7. encryption software (e.g. PGP)
8. Internet browsers (e.g. Mozilla Firefox)
9. FTP clients (e.g. FireFTP)
10. and hundreds of other types of software.

Illustrations for Computer System

Laptop computers

Cell phones

Sophisticated laser printers

Hi-end scanners

The American courts have held that the Internet falls under the definition of computer system and the use of email is accessing a computer.

State of Pennsylvania v. Murgalis

[No. 189 MDA 1999

(Pa. Super.Ct., June 2, 2000)]

Computer Network

According to section 2(1)(j) of the IT Act

"computer network" means the interconnection of one or more computers through: the use of satellite, microwave, terrestrial line or other communication media and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

The interconnection of one or more computers through:

Satellite

Satellite Internet connection is an arrangement in which the outgoing and incoming data travels through a satellite. Each subscriber's hardware includes a satellite dish

antenna and a transceiver (transmitter / receiver). The dish antenna transmits and receives signals.

Microwave

The term microwave refers to electromagnetic waves of a particular frequency. Microwave frequencies are used in radars, Bluetooth devices, radio astronomy, GSM mobile phone networks, broadcasting and telecommunication transmissions etc.

Terrestrial line

Terrestrial lines include fibre optic cables, telephone lines etc.

Other communication media

Communication media refers to any instrument or means that facilitates the transfer of data, as between a computer and peripherals or between two computers. Other ways in which two computers can be connected include cables, hubs, switches etc.

Thank you