1.3 Jurisprudence of Indian Cyber Law

> **Note:** The Act, rules, regulations, orders etc referred to in this section are discussed in more detail in the Chapter 3 titled "**Introduction to 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).

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.

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.

1.4 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.

1.4.1 Computer

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:

1. It is a high-speed **data processing device** or system.
2. It may be **electronic**, **magnetic**, **optical** etc.
3. It performs **logical**, **arithmetic**, and **memory functions**
4. These functions are performed by manipulations of electronic, magnetic or optical impulses.

Computer includes

1. all input facilities,
2. all output facilities,
3. all processing facilities,
4. all storage facilities,
5. all computer software facilities, and
6. all communication facilities

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

Let us examine the important terms used in this definition:

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.