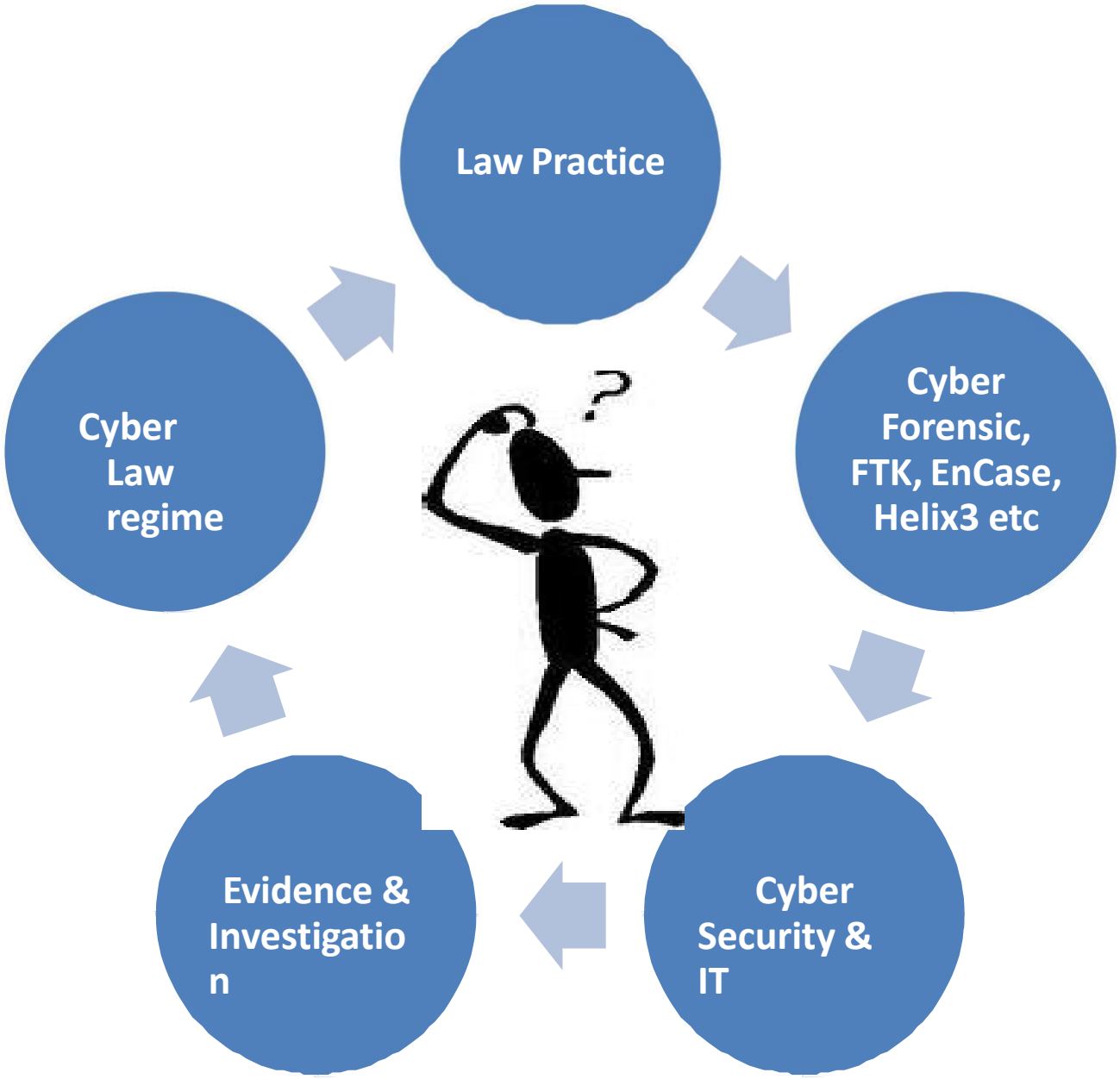
Unit VI

Cyberspace and the Law & Miscellaneous provisions of IT Act

“Cyber Law” is a vast study

- It is not the IT Act but, It includes, and is comprised of many Acts, legislations like Evidence, IPC & Cr.P.C.
- The IT Act in itself, is a challenging study.
- Understanding the difference between http & https is beyond the comprehensive capacity for any Lawyer.
- Cyber forensic, Cyber security, Cyber law, anatomy of cyber attacks ….ohhh !


Law Practice
Cyber Forensic, FTK, EnCase, Helix3 etc
Cyber Security & IT
Evidence & Investigation
Cyber Law regime

Introduction

The Information Technology Act is the Second Law in India governing the field of Technology.

The First one was in the year 1885.

That was the **Indian Telegraph Act 1885**

- However, The first recorded Cyber crime incident is believed to be recorded in the year 1820 !

- Difficult to believe ? Any guesses ?

In the year 1820, Sir Joseph-Marie Jacquard, created an automated loom.

This device was blended with analogical technology in the weaving of special fabrics.

This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology.

This was the first recorded cyber crime !

But why Cyber Law ?

Because :

- Cyber space is a completely different sphere of human existence.
- No regards for any Government or territory.
- To facilitate international norms.
- Cyber Law needs to be specific.

- Conventional Laws will muddle up the cyber law structure.

Intention of the IT Act 2000

The Act begins with :

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies…"

Two definitions of Cybercrime

- Cybercrime in a restrictive sense (Computer crime)

Any illegal behavior that is carried out by means of electronic methods targeting the security of the computer systems and data processed by them.

- Cybercrime in a general sense (Computer-related crime)

Any illegal behavior that is committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, and offering or distributing information by means of a computer system or network.

These definitions are complicated by the fact that an act may be illegal in one nation but not in another.

For example,

- Unauthorized access to computer
- Causing damage to computer data or programs
- An act of computer sabotage
- Doing unauthorized interception of communications
- Carrying out computer espionage
- Computer Tresspassing

Evolution of the Act

The General Assembly of the United Nations by its resolution A/RES/51/162, dated the 30th January, 1997 had adopted the Model Law on E - Commerce adopted by the UNCITRAL

The said resolution recommended *that* all member States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information; i.e. amongst member nations to promote international trade and commerce via electronic means.

Hence, the same was adopted and enforced in India.

UNCITRAL- United Nations Commission on International Trade Law - Role

- The official function of the UNCITRAL - modernization and harmonization of rules on international business.
- The organization is responsible for helping to facilitate international trade and investment.
- The annual sessions of UNCITRAL are held alternately in New York City and Vienna, where it is headquartered.

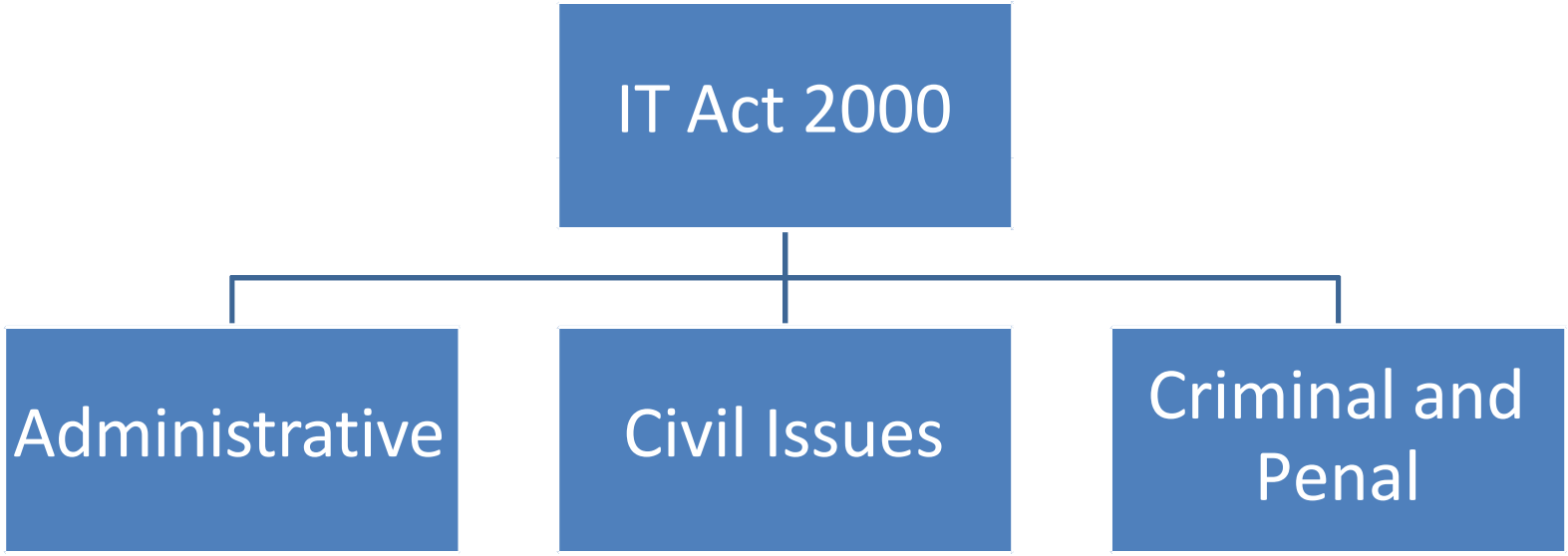
Cyber Law in India

Aided by many other Acts and Statutes.

1) The Indian Penal code
2) The Evidence Act
3) the Code of Criminal Procedure.
& many others

The Information Technology Act

- The Act can be broadly classified into 3 aspects :



IT Act of 2000

ADMINISTRATIVE PART :

- Recognizing e-commerce
- Legal enforceability and authentication of electronic - Documents
- Methodology and process.
- A special adjudicating officer & Cyber Law Appellate Tribunal
- Their role and duties therein.

IT Act 2000

The CIVIL aspect

- Runs parallel to Administrative ventures of the IT Act.
- Describes what constitutes civil infringement of rights.
- Prescribes civil duties

IT Act 2000

CRIMINAL Part

- Recognizes and provides for Penal measures against crime in cyber space, digital crimes or crime against computer resource.
- Related issues to redress, monitor, restrict, investigate, cyber crime is also provided herein.

IT Act 2000

Recognises the Cardinal Philosophy of Cyber disputes

1) Computers can be abused.

2) Computers are weapons as well as Victims.

The term “Computer” has a wide amplitude in view of the IT Act.

Definition of a Computer

- Section 2 of the Act defines :

- (i)"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.

- (j) "computer network" means the interconnection of one or more computers through—
  - (i) the use of satellite, microwave, terrestrial line
  - or other communication media; and
  - (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

- (k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

- (l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

- The new amendment also defines :

- Cyber Café (s 2 (na))
- Electronic signature (apart from DSC)
- Communication devices. (s 2 (ha))
- Cyber security (s 2 (nb))
- Indian CERT (Computer Emergency Response Team) (s 70 B (1))

Section 4- Legal recognition of Electronic Records

- If any information is required in printed or written form under any law the Information provided in electronic form, which is accessible so as to be usable for subsequent use, shall be deemed to satisfy the requirement of presenting the document in writing or printed form.

- A general provision for recognizing

Sections 5, 6, 7, 8, 9 & 10.

- 5 - Legal recognition of electronic signatures
- 6 - Use of e-Records & signatures in Government & Its Agencies
- 7 and 7 (a)- Retention of Electronic Records & audits
- 8 - Publications of rules and regulations in the e-Gazette.
- 9 - no right to claim and insist on electronic documents
- 10 – Central Govt retains the power to make rules w.r.t. e-Signatures (type, manner, format & process)

Sections 11, 12 – Receipt & Ack.

- Sec. 11 – discuss about the attributor(sender) of electronic record i.e. sender himself, or by a person authorized by the author, or by an auto response duly programmed on behalf of the author
- Sec. 12 – discuss receipt for acknowledgement where nothing has been stipulated
    - Any communication from addressee/automated or otherwise.
    - Any conduct of the addressee that proves

IT Act –overview of other relevant admin. provisions

Sec. 16	**Central Government to prescribe security procedures !!!**
Sec 17-34	Appointment and Regulation of Controller and certifying authority
Sec 35 to 39	Obtaining Digital Signature Certificate
Sec 40 to 42	Duties of Subscriber of DSC- exercise due care to retain the private key

Administrative character

Sec 44 : penalty for failure to furnish information, return etc…

- Appointment and functions of Adjudicating officer
- Powers and functioning of the Cyber Law Appellate Tribunal

- Sec 61 : Civil Court excluded from jurisdiction.
- Sec 46 & 2(1)(c) : Adjudicating officer.

Offences in a Gist

Sec 43 : earlier a simple civil provision

Now a Civil, and may amount to a penal offence u/s 66 if a fraudulent or dishonest means is established !

It relates to access to computer without the permission of the computer owner

It penalizes any sort of unauthorized access or assistance

Sec 43 in a nut shell

- **Whoever without permission of owner of the computer**
  - Secures/Disrupts access of computer ..resource..network..
  - Downloads, copies, extracts any data
  - Introduces or causes to be introduced any viruses or contaminant
  - Damages or causes to be damaged any computer resource
    - Destroy, alter, delete, add, modify or rearrange
    - Change the format of a file
  - Disrupts or causes disruption of any computer resource
    - Preventing normal continuance of computer

- Sec 43A: Failure to protect Data

Examples

- An employee authorised to access Word files, accesses internet.
- A student inadvertently spreads a virus with his USB Drive.
- A neighbor mistakenly chops off the internet cable, expecting it to be an electric wire.

Sec 65 : Tampering with Computer Source documents.

Punishment – Imprisonment upto three years or fine upto Rs 2 Lacs or both.

Sec 66 : Penalises any contravention u/s 43 if carried out with a fraudulent or dishonest motive

Punishment – Imprisonment upto three years or fine upto Rs 5 Lacs or both.

Sec 66 A : Punishment for sending offensive messages through communication service etc…

Requisites : offensive or menacing or false, or for the purpose of annoyance, inconvenience, ill will etc…

Punishment – Imprisonment upto three years and with fine.

- Sec 66 B : Punishment for dishonestly receiving stolen computer/resource etc.
- Sec 66 C : Punishes identity theft (DSC, passwords, or such unique identification.)
- Sec 66 D : Punishes personating, by means of Computer resource.
- Sec 66 E : Punishes violation of privacy rights.
- Sec 66 F : Punishes Cyber Terrorism

Sec 67A : Punishment for publishing or transmitting of material containing sexually explicit act, etc.. In the electronic form.

Punishment :

1st conviction-Imprisonment upto 5 years and fine upto Rs 10 Lacs.

2nd conviction-Imprisonment upto 7 years and fine upto Rs 10 Lacs.

EXCEPTION

Art, Science, literature or other interests of learning and other cases

Sec 67B : Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc.. In the electronic form. (Readwith other sub rules)

Punishment :

1st conviction-Imprisonment upto 5 years and fine upto Rs 10 Lacs.

2nd conviction-Imprisonment upto 7 years and fine upto Rs 10 Lacs.

Sec 67C : Preservation & retention of information by intermediaries.

Punishment - Imprisonment upto three years and with fine.

Sec 68 : Provision and punishment for violation of orders from the Controller.

Sec 69 : Powers of the Govt. to issue direction for monitoring, intercepting or decrypting any information through any Computer Resource.

(Basically an administrative right of the Govt. and provides for punishment to the violator, usually intermediaries who are incharge of such database or are service providers.)

Sec 69 A powers for blocking of public access

Sec 69 B power to authorize monitor and collect traffic.

- Sec 71 : Penalty for Misrepresentation before the Controller or the Certifying Authority
  - Punishment - Imprisonment upto 2 years or fine upto Rs. 1 Lac or both.

- Sec 72 : Penalty for breach of Confidentiality & privacy, the provision applies to those persons who are empowered under this Act with such a database or records.
  - Punishment - Imprisonment upto 2 years or fine upto Rs. 1 Lac or both.

- Sec 72A : Penalty for disclosure of information in breach of Lawful Contract –(an amendment to include even the employees of private organisations or such intermediaries working therein)
  - Punishment - Imprisonment upto 3 years or fine upto Rs. 5 Lac or both.

- Sec 74 : Publication of Signature or signature certificates for fraudulent purpose.
    - Punishment - Imprisonment upto 2 years or fine upto Rs. 1 Lac or both.

- Sec 76 : provides for confiscation of any related computer accessory, system part etc if the same is believed to be used in any violation of this Act or rules.

- Sec 77 B : Offences punishable with imprisonment upto 3 years to be bailable.

- Sec 78 : Power to investigate offences now available to Inspector, earlier the onus was on the DSP rank officer or above.

- Sec 79 : Exemption of Intermediaries and service providers if they establish that they have exercised due diligence on their part.

- An abusive provision for the ISP's but often helpful !

- The 2009 notification makes it an offence to even abet or attempt a cyber crime, earlier unsuccessful criminals always escaped by virtue of this grey area.

- Sec 84 B : Punishment for Abetment
  - Same punishment as prescribed for the offence

- Sec 84 C :Punishment for attempt
  - A maximum of one-half of the term of imprisonment provided for the offence, or with fine as prescribed for the offence or with both.

- Sec 90: State Govt. has powers to make allied rules.

Relevant application of IPC etc…

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forging electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act
Web - Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

Weak Areas of the ITA 2000

- It causes a conflict to the jurisdiction.
- Not having defined rule for Domain Names.
- Intellectual Property Rights are not addressed.
- Not covering privacy and content regulation.
- Electronic Payment is also not covered wisely in the act.

Cybercrime: Examples and Mini-Cases

- Official Website of Maharashtra Government Hacked
- Indian Banks Lose Millions of Rupees
- Parliament Attack
- Pune City Police Bust Nigerian Racket
- e-mail spoofing instances

Mini Cases

- The Indian Case of online Gambling
- An Indian Case of Intellectual Property Crime
- Financial Frauds in Cyber Domain