INFORMATION TECHNOLOGY ACT, 2000 [As Amended by Information Technology (Amendment) Act 2008]

K S SCHOOL OF BUSINESS MANAGEMENT

Prof. Amishi Shah
M.Com, LLM

IT ACT, 2000

- The IT Act was enacted in August, 2000 and it was amended in 2008 and now it is **IT (Amendment) Act, 2008**. The IT Act, 2000 is based on the Model Law of E-Commerce adopted by UNCITRAL in 1996.
- IT Act, 2000 consists of
- 90 Sections divided into 13 chapters and 4 Schedules.
- It shall **extend to the whole of India** and, save as otherwise provided in this Act, it applies also to any **offence or contravention hereunder committed outside India by any person**.

Amendment Act 2008

- Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient.
- There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.
- Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations.

- Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October, 2009.

Some of the notable features of the ITAA are as follows:

- ❑ Focusing on data privacy
- ❑ Focusing on Information Security
- ❑ Defining cyber café
- ❑ Making digital signature technology neutral
- ❑ Defining reasonable security practices to be followed by corporate
- ❑ Redefining the role of intermediaries
- ❑ Recognizing the role of Indian Computer Emergency Response Team
- ❑ Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- ❑ authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

IT ACT ADDRESSES THREE AREAS

- **The IT Act essentially seeks to address three areas or perceived requirements for the digital era:**

(a) to **make possible e-commerce transactions**—both business to business and business to consumer

(b) to **make possible e-governance transactions**—both government to citizen and citizen to government

(c) to **curb cyber crime and regulate the Internet.**

MAIN OBJECTIVES OF THE IT ACT

- To provide legal **recognition for electronic transactions**
- To **facilitate electronic filing** of documents with **Govt. agencies**
- To **amend certain Acts** such as

➢Indian Penal Code, 1860; - 1st schedule

➢Indian Evidence Act, 1872; - 2nd schedule

➢The Banker's Book Evidence Act, 1891 and

➢The Reserve Bank Of India Act, 1934

- To provide **legal framework and legal sanctity to electronic records** and other activities carried out electronically
- To give legal **validity and enforceability to electronic contracts**

- To **appoint Certifying Authorities for issuing digital signature** and to **provide regulatory regime** by implementing **civil and criminal liabilities** on person's contravening the provisions of the Act
- To **confer powers on the Central Government** for **appointing adjudicating officers** vested with powers of a civil court for adjudicating cases related to contraventions of the provisions of the Act
- IT Act, 2000 was amended in 2008 as new crimes, new methods for committing them cropped up. The amended Act included **new cyber offences** and cleared the grey areas which were there in the previous Act. The IT (amendment) Act, 2008 as brought marked change in the IT Act 2000 on several counts.

LIMITATION OF IT ACT

- Foreign Certifying Authorities were recognise under Sec 19 of the Act
- Certain drawbacks were identified in these section
- When the Foreign Certifying Authority are already recognised, then it is embarrassing to ask them to obtain license from the Central Government once again
- It is observed that Foreign Certifying Authorities should be subjected to licensing only if they want to issue digital certificates to individuals or companies in India
- Provided the Foreign Company, which does not presently have recognition in any other country, wants to set up digital certificate service in India, such companies may be subjected to prior approval of the government and gazette notification

Despite its expansive scope, The IT Act omits several important issues.

- The provisions of the ITA are not applicable to

1. **a negotiable instrument** as defined in section 13 of the Negotiable Instruments Act, 1881;
2. **a power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
3. **a trust** as defined in section 3 of the Indian Trusts Act, 1882;
4. **a will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
5. **any contract for the sale or conveyance of immovable property or any interest in such property**;
6. **any such class of documents or transactions as may be notified by the Central Government** in the Official Gazette.

- The ITA only recognises the Public Key Information (PKI) frame work for authentication and **does not recognise any other form of authentication procedure**
- Search and Arrest powers conferred on Police Officers are specific to public places, while **no guidelines are provided for such powers in other locations.** Since Cyber Crime more often occurs in the privacy of ones' home or office, more specific regulations are needed to address this issue
- No provisions in the ITA deal with **protecting intellectual property** rights or copyright violations over the internet
- No mention is made of **taxation issues** relative to the internet

CHAPTERS UNDER IT ACT

I. PRELIMINARY (Sec 1- 2)

Ii. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (Sec 3-4)

III. ELECTRONIC GOVERNANCE (Sec 4-10)

IV. ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS (Sec 11-13)

V. SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES (Sec 14-16)

VI. REGULATION OF CERTIFYING AUTHORITIES ELECTRONIC SIGNATURE CERTIFICATES (Sec 17-34)

VII. ELECTRONIC SIGNATURE CERTIFICATES (Sec 35-39)

VIII. (Sec 40-42)

IX. PENALTIES , COMPENSATION AND ADJUDICATION (Sec 43- 47)

X. THE CYBER APPELLATE TRIBUNAL (Sec 48 – 64)

XI. OFFENCES (Sec 65 – 78)

XII. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES (Sec 79)

XII A . EXAMINER OF ELECTRONIC EVIDENCE (Sec 79A)

Xiii. MISCELLANEOUS (Sec 80 – 90)

SALIENT FEATURES OF THE IT ACT, 2000

- The Act extends to the whole of India (Sec 1)
- Sec 3 of the Act provides for authentication of electronic records, legal frame work for affixing digital signature by use of asymmetric crypto system and hash functions
- Sec 4 of the Act provides legal recognition of electronic records
- Sec 5 gives legal recognition to the digital signature
- Retention of electronic record Sec 7
- Publication of official gazette in electronic form Sec 8
- Sec 14,15,16 provides security provisions for electronic record and digital signature

- Sec 17 to 42 provide for licensing and recognition of certifying authority for issuing digital signature certificate
- Sec 18 enumerates functions of controller
- Sec 19 empowers for appointment of certifying authority and controller of certifying authority including recognition of foreign certifying authority
- Sec 20 authorises controller to act as repository of all digital signature certificate
- Sec 43 and 66 gives data protection
- Sec 43 and Sec 66, 67 and 72 define various types of computer crimes and prescribe stringent penalties under the Act
- Sec 46 and 47 provide for appointment of adjudicating officer for judgement inquiries under the Act

- Sec 48 to 56 establish Cyber Appellate Tribunal under the Act
- Sec 57 provides procedure for appeal from order of adjudicating officer to cyber appellate tribunal and not to any Civil Court
- Appeal from order of Cyber Appellate Tribunal to High Court (Sec 62)
- Sec 69 provides for interception of information from computer to computer
- Protection system Sec 70
- Sec 75 of the Act applies for offences or contraventions committed outside India
- Sec 76 empowers DSP (Deputy Superintendent of Police) for investigation of computer crimes
- Network service provider not to be liable in certain cases Sec 79

- Sec 80 states the power of police officer and other officers to enter in to any public place and search and arrest without warrant
- Offences by the companies Sec 85
- Constitution of Cyber Regulations Advisory Committee who will advise the Central Government and Controller Sec 88

- **New provisions added though 2008 amendments**

- Sec 3A is inserted to address technology neutrality from its presence technology specific form i.e. Digital Signature to Electronic Signature
- Sec 6A – promotion of e-governance and other IT applications such as delivery of service, outsourcing, public private partnership

- Sec 10A validate electronic contracts
- Sec 43 data protection and privacy
- Sec 43A and 72A – body corporate and to implement best security practise
- Sec 49 to 52 – to establish multi member Appellate Tribunal
- Sections to address new form of computer misuse
  - impersonation section 419A
  - identity theft and e commerce fraud like phishing under section 417A
  -Video voyeurism Sec 502A
  - offensive messages and spam section 66A
  - Pornography Sec 67A
- Preservation and retention of Data Sec 67C

- Sec 69A – blocking information for public access
- Monitoring of traffic data and information for Sec 69B cyber security
- Sec 70A designates agency for protection of critical information infrastructure
- Sec 70B prescribes power of CERT – in to call and analysis information relating to breach in cyber space and cyber security
- Sec 79 regulates cyber cafes
- Punishment for most of offences were reduced from 3 years to 2 years

Sec - 2 Definitions

- Sec 2(f) "**Asymmetric Crypto System**"

means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

- Sec 2(ha) "**Communication Device**"

means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

- Sec2(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

- Sec 2(j) "**Computer Network“**

means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

- Sec 2(k) **"Computer Resource"**

means computer, communication device, computer system, computer network, data, computer database or software;

- Sec 2(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;

- Sec 2(na)"**Cyber cafe"**

means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

- Sec 2(nb)"**Cyber Security"**

means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

- Sec 2(p) **"Digital Signature"**

means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

- Sec 2(t) **"Electronic Record"**

means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

- Sec 2(ta)“**Electronic Signature"**

means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

- Sec 2(zc) **"Private Key"**

means the key of a key pair used to create a digital signature;

- Sec 2(zd) **"Public Key"**
- means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
- Sec 2(ze) **"Secure System"**

means computer hardware, software, and procedure that -:

(a) are reasonably secure from unauthorized access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

SIGNATURE

- **American Bar Association defines Signature** as :

The name of a person or a mark or sign representing his name, marked by himself or by an authorized deputy.

The act of signing one's name

A distinctive mark, characteristic that identifies a person or thing

A legal signature is the mark of a specific individual against a specific document at a specific time given with specific intent.

- **Signature are of three types**

➢ Handwritten signature

➢ Electronic signature

➢ Digital signature

DIGITAL SIGNATURE

- In the present digital world, individuals are mostly not communicating with each other unlike in physical space but are communicating in anonymous cyberspace
- Thus much **emphasis is placed on authentication of electronic information** and hence there was a need for a secure authentication tool and hence it led to evolution of digital signature
- A digital signature is **essentially to identify the signatory** by linking the signatory with the content of a document and to provide certainty about the signatory's personal participation in signing
- It also helps to **demonstrate the intention** of the signatory to endorse or approve authorship of a text and the fact that the signatory had been at a given place and time

- In a digital system, an adopted method must ensure that the document signed are not subject to forgery and enable a party to sell a signed message to another in such a way that the **following conditions are fulfilled**

➢The receiver can confirm the identity of the claimed sender

➢The sender can not later repudiate the contents of the message

➢The receiver is not expected to have fabricated the message himself

- Digital signature can be **used anywhere where a system for authenticating data is necessary**
- A system of digital signatures and encryption is used in e-commerce to protect confidential information
- Digital signature **facilitate different people and different organisations in many different sectors**

DIGITAL SIGNATURE

A **digital signature** is an electronic scheme for demonstrating the authenticity of a digital message or document.

A valid digital signature gives recipient a reason to believe that the message was created by a known sender and that it was not altered in transit.

Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect imitation or tampering.

Authentication of Digital Signature

A digital signature shall –

- be created and verified by cryptography that concerns itself with transforming electronic records.

- use "Public Key Cryptography" which employs an algorithm using two different mathematical "keys" – one for creating a digital signature or transforming it and another key for verifying the signature or returning the electronic record to original form. Hash function shall be used to create this signature. Software utilizing such keys are termed as "asymmetric cryptography" [Rule 3 of IT Rules, 2000].

Digital signatures can be used to authenticate the source of messages.

When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is obvious in a financial context.

For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Verification of Digital Signature

Verification means to determine whether –

- the initial record was affixed with the digital signature by using the "keys" of the subscriber.
- the original record is retained intact or has been altered since such electronic record was bounded with the digital signature [Sec.2(1)(zh)].

DIGITAL SIGNATURE CERTIFICATE

A **digital signature certificate** is an electronic document which uses a digital signature to bind an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that it belongs to an individual.

Any person can make an application to the Certifying Authority for the issue of this digital certificate. The Authority charges fees (as prescribed by the Central Government) for the issue of "digital signature certificate".

Generation of Digital Certificate

The generation of digital signature certificate shall involve –

- ❑ receipt of an approved and verified certificate request.
- ❑ creating a new digital signature certificate.
- ❑ a distinguished name associated with the digital certificate owner.
- ❑ a recognized and relevant policy as defined in certification practice statement [Rule 24 of the IT rules].

Compromise of Digital Certificate

Digital signature certificate shall be deemed to be compromised where the integrity of –

- the key associated with the certificate is in doubt.
- the certificate owner is in doubt, as to the attempted use of his key pairs, or otherwise for malicious or unlawful purposes.

The digital certificate shall remain in the compromise state for only such time as it takes to arrange for revocation.

Expiry of Digital Signature Certificate

- A digital signature certificate shall be issued with a designated expiry date. It will expire automatically and on expiry, it shall not be re-used. The period for which a digital certificate has been issued shall not be extended, but a new digital signature certificate may be issued after the expiry of such period [Rules 26 of IT Act, 2000].

- **Digital signature are helpful in authenticating one's online**
  - Medical records
  - Financial transactions such as bank transfers, IT fillings, etc.
  - Education online courses registration
- **Business people use digital signature for authorising**
  - Financial transactions such as securities trading
  - Business discussions like company mergers etc.
  - Communication of trade secrets
  - Filing of legal document
- **Government uses the digital signature for**
  - Validating military information
  - Voting (registration, online voting etc.)

ELECTRONIC SIGNATURE

- **Electronic signature is defined** as “any symbol or method adopted by a party in the process of validation provided there ease and existing intention to be bonded by or to authenticate a record accompanied by electronic means.”
- Electronic signature is **not limited to any type of digital marking** used by a party to be bond to or to authenticate a record but also include marking as diverse as **digitalised image of paper signatures**
- It can be a **typed notation**, which is affixed at the bottom of an electronic document or even addressing notation such as **electronic mail header or footers**
- An electronic signature is a digitized hologram or a **digital signature** system using public key infrastructure or nay process employed to authenticate an electronic record i.e. transmitted or stored electronically

ELECTRONIC VS DIGITAL SIGNATURE

- **Electronic signature is defined** as, any identifier such as letters, characters or symbols manifested by electronic or similar means, executed or adopted by a party to a transaction with an intent to authenticate writing
- **Digital signature** is an electronic identifier that utilises an information security measure, most commonly cryptography, to ensure the integrity, authenticity and non-repudiation of the information to which it corresponds

- **Electronic signature** is a generic term that refers to any representation in electronic form which expresses intent, including a printed name at the bottom of an email, a digitalised copy of an hand written signature, biometric mark or a sound or a digital signature
- **Digital signature** is a specific type of electronic signature based on public key cryptography, used within a framework known as public key infrastructure (PKI)
- Electronic signature are **technology neutral**
- Digital signature are **technology specific**
- **Digital signature is one of the type of electronic signature** but the later is a broader concept than the former
- **Electronic signature possesses all technology** which replace hand written signature in an electronic environment and include every way of authenticating data by means of information technology
- **Digital signature is a name for technology applications** using asymmetric cryptography to ensure the authenticity of electronic messaging and guarantee the integrity of the contents of these messages

- **Electronic signature has no way of verifying** weather a document has been altered from the time it was signed and does not provide any kind of signatory or document authentication
- **Digital signature** based on public key system provide for signatory or document authentication and also non-repudiation
- **Electronic signature** are the electronic equivalent of a signature on a conventional contract, capable of joining two parties in a legal binding agreement
- **Digital signature** are placed on specific data such as email, web request or web page which is used to verify that the data has emanated from the claim source

E-governance implies action and commitment of the state and its agencies at two levels:

(a) It involves the **promotion** of the information and **communication technologies** and, especially, e-commerce, on the one hand, and

(b) The **adopting of these technologies** and all they involve in the matter of a completely new type of commitment, open systems and use of the medium of the Internet for government business, citizen interaction, and most important, for development.

But when it comes to laying down of specific rules with respect to the basic essential ingredients of a contract in the sphere of e contracts the laws are **not extensive enough to include each and every aspects of a valid contract.**

ELECTRONIC GOVERNANCE

- **Sec 4 Legal Recognition of Electronic Records**

Where any law provides that information or any other matter **shall be in writing or in the typewritten or printed form**, then, notwithstanding anything contained in such law, such **requirement shall be deemed to have been satisfied** if such information or matter is

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

- **Sec 5 Legal recognition of Electronic Signature**

Where any law provides that information or any other matter shall be **authenticated by affixing the signature** or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such **requirement shall be deemed to have been satisfied**, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

- **Sec 6 Use of Electronic Records and Electronic Signature in Government and its agencies**

(1) Where any law provides for

(a) the **filing of any form**, application or any other document with any office, authority, body or agency owned or **controlled by the appropriate Government** in a particular manner;

(b) the **issue or grant of any license, permit, sanction or approval** by whatever name called in a particular manner;

(c) the **receipt or payment of money in a particular** manner, then, notwithstanding anything contained in any other law for the time being in force, such **requirement shall be deemed to have been satisfied** if such filing, issue, grant, receipt or payment, as the case may be, is effected by **means of such electronic form** as may be prescribed by the appropriate Government.

- **Sec 7 Retention of Electronic Records**

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be **deemed to have been satisfied** if such documents, records or information are retained in the electronic form, -

(a) the information contained therein **remains accessible** so as to be usable for a **subsequent reference**;

(b) the electronic record **is retained in the format** in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will **facilitate the identification** of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

- Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- **Sec 10A Validity of contracts formed through electronic means**

Where in a **contract formation**,

the **communication of proposals**,

the **acceptance of proposals**,

the **revocation of proposals and acceptances**, as the case may be,

are **expressed in electronic form** or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

- **Sec 11 Attribution of Electronic Records**

An electronic record shall be attributed to the originator

(a) if it was sent by the **originator himself**;

(b) by a person who had the **authority to act on behalf of the originator** in respect of that electronic record; or

(c) by an **information system programmed** by or on behalf of the originator to operate automatically.

- **Sec 12 Acknowledgement of Receipt**

(1) Where the originator has **not agreed with stipulated that the acknowledgment** of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -

(a) any **communication by** the addressee, automated or otherwise; or

(b) any **conduct of** the addressee, sufficient to indicate to the originator that the electronic record has been received.

- (2) Where the **originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment** of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
- (3) Where the originator has **not stipulated that the electronic record shall be binding only on receipt of such acknowledgment**, and the acknowledgment has not been received by the originator **within the time specified** or agreed or, if **no time has been specified** or agreed to within a **reasonable time**, then the originator **may give notice** to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if **no acknowledgment is received within the aforesaid time limit he may after giving notice** to the addressee, treat the electronic record as though it has **never been sent**.

- **Sec 13 Time and place of despatch and receipt of electronic record**

(1) Save as otherwise agreed to between the originator and the addressee, the **dispatch** of an electronic record occurs when it **enters a computer resource outside the control of the originator**.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely –

(a) if the addressee **has designated a computer resource** for the purpose of receiving electronic records

(i) receipt occurs at the time when the electronic record enters the **designated computer resource; or**

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the **electronic record is retrieved by the addressee;**

(b) if the addressee has **not designated a computer resource along with specified timings**, if any, receipt occurs when the **electronic record enters the computer resource of the addressee**.

- (3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to "be **dispatched at the place** where the originator has his **place of business**, and is deemed to be received at the place where the addressee has his place of business.
- (4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
- (5) For the purposes of this section –

(a) if the originator or the addressee has more than one place of business, **the principal place of business** shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his **usual place of residence** shall be deemed to be the place of business;

(c) "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

REGULATION OF CERTIFYING AUTHORITIES

- **Sec 17 Appointment of Controller and other officers**

(1) The **Central Government** may, by notification in the Official Gazette, **appoint a Controller of Certifying Authorities** for the purposes of this Act and may also by the same or subsequent notification **appoint such number of Deputy Controllers and Assistant Controllers**, **other officers and employees** (Inserted vide ITAA 2008) as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

- **Sec 18 The Controller may perform all or any of the following functions**, namely

(a) exercising **supervision** over the **activities of the Certifying Authorities**;

(b) **certifying public keys** of the Certifying Authorities

(c) laying down the **standards to be maintained** by the Certifying Authorities;

(d) specifying the **qualifications and experience which employees of the Certifying Authorities** should possess;

(e) specifying the **conditions subject to which the Certifying Authorities shall conduct** their business;

(f) specifying the **content of written, printed or visual material and advertisements that may be distributed** or used in respect of a Electronic Signature Certificate and the Public Key;

(g) **specifying the form and content of a Electronic Signature Certificate** and the key;

(h) specifying the form and manner in which **accounts shall be maintained** by the Certifying Authorities;

(i) specifying the terms and conditions subject to which **auditors may be appointed** and the remuneration to be paid to them;

(j) facilitating the **establishment of any electronic system** by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the **manner in which the Certifying Authorities shall conduct their dealings** with the subscribers;

(l) **resolving any conflict of interests** between the Certifying Authorities and the subscribers;

(m) laying down the **duties of the Certifying Authorities**;

(n) **maintaining a data-base containing the disclosure record** of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

- **Sec 19 Recognition of foreign Certifying Authorities**

(1) Subject to such conditions and restrictions as may be specified by regulations, the **Controller may with the previous approval of the Central Government**, and by notification in the Official Gazette, **recognize any foreign Certifying Authority** as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may if he is satisfied that **any Certifying Authority has contravened any of the conditions and restrictions** subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, **revoke such recognition.**

- **Sec 21 License To Issue Electronic Signature Certificates**

any person may make an **application**, to the Controller, for a **license to issue Electronic Signature Certificates**, unless the applicant fulfils such **requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities**, which are necessary to issue Electronic Signature Certificates as may be prescribed by the Central Government.

A **license granted** under this section shall –

(a) be **valid for such period as may be prescribed** by the Central Government;

(b) **not be transferable or heritable**;

(c) be subject **to such terms and conditions** as may be specified by the regulations.

- **Sec 23 Renewal Of License**

An application for renewal of a license shall be –

(a) in such form;

(b) accompanied by such **fees**, **not exceeding five thousand rupees**, as may be prescribed by the Central Government and shall be made **not less than forty-five days before the date of expiry** of the period of validity of the license

- **Sec 24 Procedure for grant or rejection of license**

The Controller may, on receipt of an application, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

Provided that **no application shall be rejected** under this section **unless the applicant has been given a reasonable opportunity of presenting his case.**

- **Sec 25 Suspension of License**

(1) The Controller may, if he is **satisfied after making such inquiry**, as he may think fit, that a Certifying Authority has –

(a) made a statement in, or in relation to, the **application** for the issue or renewal of the license, which is **incorrect or false in material particulars**;

(b) **failed to comply with the terms and conditions** subject to which the license was granted;

(c) **failed to maintain the standards**

(d) **contravened any provisions** of this Act, rule, regulation or order made there under, revoke the license:

Provided that no license shall be revoked unless the Certifying Authority has been given a **reasonable opportunity of showing cause** against the proposed revocation.

- **Sec 26 Notice of suspension or revocation of license.**

Where the license of the Certifying Authority is suspended or revoked, the Controller shall **publish notice of such suspension or revocation**, as the case may be, in the **data-base maintained by him.**

- **Sec 27 Power to delegate**.

The Controller may, **in writing, authorize the Deputy Controller**, **Assistant Controller or any officer** to exercise any of the powers of the Controller under this Chapter

- **Sec 28 Power to investigate contraventions.**

(1) **The Controller or any officer authorized** by him in this behalf shall **take up for investigation** any contravention of the provisions of this Act, rules or regulations made there under.

(2) The Controller or any officer authorized by him in this behalf shall **exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961** and shall exercise such powers, subject to such limitations laid down under that Act.

- Sec 29 Access to computers and data.
- Sec 30 Certifying Authority to follow certain procedures
- Sec 31 Certifying Authority to ensure compliance of the Act, etc
- Sec 32. Display of license.

Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.

- Sec 33 Surrender of license
- Sec 34 Disclosure (as required)

ELECTRONIC SIGNATURE CERTIFICATES

- **Sec 35 Certifying Authority to issue Electronic Signature Certificate**

(1) **Any person** may make an **application to the Certifying Authority** for the **issue of a Digital Signature Certificate** in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such **fee not exceeding twenty-five thousand rupees** as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be **accompanied by a certification practice statement** or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, **after consideration of the certification practice statement** or the other statement under sub-section (3) and **after making such enquiries** as it may deem fit, **grant the Digital Signature Certificate** or for reasons to be recorded in writing, reject the application

Provided that **no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection**.

- **Sec 36. Representations upon issuance of Digital Signature Certificate**

A Certifying Authority while issuing a Digital Signature Certificate shall certify that –

(a) it has **complied with the provisions of this Act** and the rules and regulations made there under;

(b) it has **published the Digital Signature Certificate** or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the **subscriber holds the private key corresponding to the public key**, listed in the Digital Signature Certificate;

(ca) the **subscriber holds a private key which is capable of creating a digital signature**

(cb) the **public key** to be listed in the certificate can be **used to verify a digital signature** affixed by the private key held by the subscriber

(d) the **subscriber's public key and private key constitute a functioning key pair**;

(e) **the information** contained in the Digital Signature Certificate is **accurate**; and

(f) it **has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the** reliability of the representations made in clauses (a) to (d).

- Sec 37. Suspension of Digital Signature Certificate.
- Sec 38. Revocation of Digital Signature Certificate
- Sec 39. Notice of suspension or revocation
- Sec 40 Generating Key Pair
- Sec 40A Duties of subscriber of Electronic Signature Certificate
- Sec 41 Acceptance of Digital Signature Certificate
- Sec 42 Control of Private key

IX. PENALTIES , COMPENSATION AND ADJUDICATION

- **Sec 43 Penalty and Compensation for damage to computer, computer system, etc**

If any person **without permission of the owner** or any other person who is incharge of a computer, computer system or computer network -

(a) accesses or secures **access to such computer, computer system or computer network or computer resource**

(b) **downloads, copies or extracts any data, computer data base** or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be **introduced any computer contaminant or computer virus** into any computer, computer system or computer network;

(d) damages or causes to be **damaged any computer, computer system or computer network, data, computer data base** or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or **causes disruption of any computer, computer system or computer network**;

(f) denies or **causes the denial of access to any person authorised** to access any computer, computer system or computer network by any means;

(g) provides any **assistance to any person to facilitate access** to a computer, computer system or computer network **in contravention** of the provisions of this Act, rules or regulations made thereunder,

(h) charges the services availed of by a person to the account of another person **by tampering** with or manipulating any computer, computer system, or computer network,

(i) **destroys, deletes or alters any information** residing in a computer resource or diminishes its value or utility or affects it injuriously by any means

(i) **Steals, conceals, destroys or alters** or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be **liable to pay damages** by way of compensation **not exceeding one crore rupees to the person so affected.**

- **Sec 43A - Compensation for failure to protect data**

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is **negligent in implementing and maintaining reasonable security practices** and procedures and thereby causes **wrongful loss or wrongful gain** to any person, such body corporate shall be **liable to pay damages** by way of compensation, **not exceeding five crore rupees, to the person so affected.**

- **Sec 44 Penalty for failure to furnish information, return, etc**

If any **person who is required** under this Act or any rules or regulations made thereunder to -

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be **liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure**;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations, **fails to file return or furnish** the same within the time specified therefore in the regulations, he shall be **liable to a penalty not exceeding five thousand rupees for every day during which such failure continues**:

(c) maintain books of account or records, **fails to maintain** the same, he shall be **liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues**.

- **Sec 45 Residuary Penalty**

Whoever **contravenes any rules or regulations** made under this Act, **for the contravention of which no penalty has been separately provided**, shall be **liable to pay** a compensation **not exceeding twenty-five thousand rupees to the person** affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

THE CYBER APPELLATE TRIBUNAL (CAT)

- The **main objective** of establishment of Cyber Appellate Tribunal is **speedy disposal of disputes**
- Chapter X of the Act discusses the establishment, composition, jurisdiction and powers of the Tribunal
- CAT is established under Sec 48 of the Act
- Sec 49 of the Act gives the composition of CAT
- Sec 50-52 provide for qualification, term of office, condition of service, salary and allowances

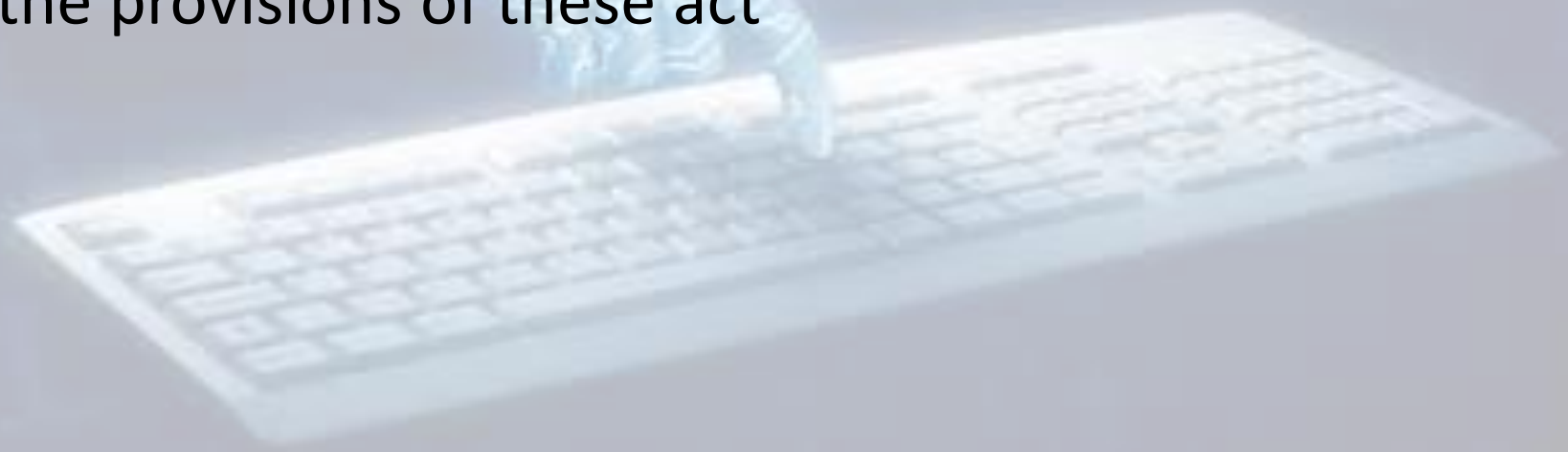
- The Tribunal is **guided by the principals of natural justice** but not either by civil procedure code or criminal procedure code
- Cyber Appellate Tribunal has the **powers to regulate its own procedure**
- The 2008 amendment of the Act **mandates that the preceding officers** of CAT shall be **appointed from amongst the persons having knowledge and professional experience** in Information Technology, Tele Communication, Industry and Management or Consumer Affairs
- The **appeal lies to CAT** against the order of the controller or adjudicating officer.
- From CAT further **appeal lies to High Court** on the question of Fact or Law

CYBER CRIME

- Cyber crime is an **emerging issue** that correspondents with the improvement and expansion of the internet
- Apart from the **individual law suits, public interest litigation (PIL)** is an important and viable **legal method** in India for ensuring justice and protecting the General public against Cyber Crime
- Since the enactment of the ITA, several PIL lawsuits have been filed addressing issues, such as online child pornography and internet fraud
- With increased awareness among the masses about online crimes and offences, a significant rise in the number of lawsuits is observed
- These PILs will serve as a powerful tool to curb online cyber crimes
- In India, The National Association of Software and Service Companies (NASSCOM) is working in association with the Ministry of Information Technology to fight such Cyber Crimes
- A significant portion of the Indian IT Act, 2000 is dedicated to adjudication, liability and defining the powers of The Cyber Regulation Appellate Tribunal (CRAT)

CHAPTER XI – ASPECTS OF CYBER CRIME

- These chapter cover within its ambit unauthorised access, hacking, obscenity, misrepresentation and breach of confidentiality, privacy and fraud
- One of the remarkable feature of this chapter is Sec -75
- This section gives an extra territorial effect to offences in contravention to the provisions of these act



- **Sec 65 Tampering with Computer Source Documents**

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be **punishable with imprisonment up to three years**, or with **fine** which may extend up to **two lakh rupees**, or with **both.**

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

- **Sec 66 Computer Related Offences (Substituted vide ITAA 2008)**

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be **punishable with imprisonment** for a term which may **extend to two three years** or with **fine** which may extend to **five lakh rupees** or with **both**.

Explanation: For the purpose of this section,-

- a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
- b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

- **Sec 66 A Punishment for sending offensive messages through communication service, etc.**

Any person who sends, by means of a computer resource or a communication device,-

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be **punishable** with **imprisonment** for a term which may extend to **two three years and with fine.**

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

- **Sec 66 B Punishment for dishonestly receiving stolen computer resource or communication device**

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be **punished with imprisonment** of either description for a term which may **extend to three years** or with **fine** which may extend **to rupees one lakh** or with **both**.

- **Sec 66C Punishment for identity theft.**

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be **punished with imprisonment** of either description for a term which may **extend to three years** and shall also be liable to **fine** which may **extend to rupees one lakh.**

- **Sec 66D Punishment for cheating by personation by using computer resource**

Whoever, by means of any communication device or computer resource cheats by personation, shall be **punished with imprisonment** of either description for a term which may **extend to three years** and shall also be liable to **fine** which may **extend to one lakh rupees**.

- **Sec 66E. Punishment for violation of privacy. (Inserted Vide ITA 2008)**

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be **punished with imprisonment** which may **extend to three years** or with fine **not exceeding two lakh rupees**, or with **both**

Explanation.- For the purposes of this section—

(a) —transmit‖ means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) —capture‖, with respect to an image, means to videotape, photograph, film or record by any means;

(c) —private area‖ means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) —publishes‖ means reproduction in the printed or electronic form and making it available for public;

(e) —under circumstances violating privacy‖ means circumstances in which a person can have a reasonable expectation that—

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

- **Sec 66F. Punishment for cyber terrorism**

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be **punishable with imprisonment which may extend to imprisonment for life'.**

- **Sec 67 Punishment for publishing or transmitting obscene material in electronic form**

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be **punished on first conviction** with **imprisonment** of either description for a term which may **extend to two three years** and with **fine** which may **extend to five lakh rupees** and in the **event of a second or subsequent conviction** with **imprisonment** of either description for a term which may **extend to five years** and also with **fine** which may **extend to ten lakh rupees**.

- **Sec 67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form**

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be **punished on first conviction** with **imprisonment** of either description for a term which may **extend to five years** and with **fine** which may extend to **ten lakh rupees** and in the event of **second or subsequent conviction** with **imprisonment** of either description for a term which may **extend to seven years** and also with **fine** which may **extend to ten lakh rupees.**

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

- **Sec 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.**

Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be **punished on first conviction** with imprisonment of either description for a term which may **extend to five years** and with a **fine** which may **extend to ten lakh rupees** and in the event of **second or subsequent conviction** with **imprisonment** of either description for a term which may **extend to seven years** and also with **fine** which may **extend to ten lakh rupees**:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years

- **Sec 67 C Preservation and Retention of information by intermediaries**

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be **punished with an imprisonment** for a term which may **extend to three years** and shall also be **liable to fine.**

- 68 Power of Controller to give directions
- 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
- 69 A Power to issue directions for blocking for public access of any information through any computer resource
- 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
- 70 Protected system
- 70 A National nodal agency
- 70 B Indian Computer Emergency Response Team to serve as national agency for incident response

- **Sec 71 Penalty for misrepresentation**

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be **punished with imprisonment** for a term which may **extend to two years**, or with **fine** which may **extend to one lakh rupees, or with both.**

- **Sec 72 Breach of confidentiality and privacy**

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be **punished with imprisonment** for a term which may **extend to two years**, or with **fine** which may **extend to one lakh rupees, or with both**

- **Sec 72 A Punishment for Disclosure of information in breach of lawful contract**

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be **punished with imprisonment** for a term which may **extend to three years,** or with a **fine** which may **extend to five lakh rupees, or with both.**

- **Sec 73 Penalty for publishing electronic Signature Certificate false in certain particulars**

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

(2) Any person who contravenes the provisions of sub-section (1) shall be **punished with imprisonment** for a term which may **extend to two years**, or with **fine** which may **extend to one lakh rupees**, or with **both**

- **Sec 74 Publication for fraudulent purpose**

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be **punished with imprisonment** for a term which may **extend to two years**, or with **fine** which may **extend to one lakh rupees, or with both**

LIABILITY OF NETWORK SERVICE PROVIDERS SEC 79

- The Act makes intermediaries like Network Service Providers liable in certain cases which provides that :
- No person providing any service as a network service provider shall be liable under this Act, rules or regulation made there under for any third party information or data made available by him if he proves that the offense or contravention was committed without his knowledge or that he had exercised all due diligences to prevent the commission of such offense or contravention
- Thus a plain reading of the section indicates that if the Network Service Provider is unable to prove its innocence or ignorance, it will be held liable for the crime

THANK YOU

ALL THE BEST