10

INFORMATION TECHNOLOGY (AMENDED) ACT, 2008

LEARNING OBJECTIVES:

- To know about IT Act 2000 (as Amended by Information Technology (Amendment) Act 2008), and its objectives
- To understand its scope and definitions
- To discuss various chapters of the Act.

10.0 BRIEF HISTORY

New communication systems and digital technology have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware of the advantages which the electronic form of business provides, people are reluctant to conduct business or conclude and transaction in the electronic form due to lack of appropriate legal framework. Electronic commerce eliminates need for paper based transactions. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance, are the requirements of writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate e-commerce, the need for legal changes has become an urgent necessity.

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. The legal recognition to electronic records and digital signatures in turn will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999.

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India. Therefore, it is important to understand 'what are the various perspectives of the IT Act, 2000 and what it offers?'.

The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic

means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

This Act was amended by *Information Technology Amendment Bill 2006*, passed *in Loksabha on Dec 22nd and in Rajyasbha on Dec 23rd of 2008.* The then Hon'ble Minister of Communications & IT, Mr. Dayanidhi Maran discussed the statement of Objects and Reasons for ITAA-2006, which are given as follows:

- The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.
- With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as a protected system so as to restrict its access.
- A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.
- The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of the United Nations by its resolution No. 56/80, dated 12th December, 2001, recommended that all States accord favorable consideration to the said Model Law on Electronic Signatures. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonization with the said Model Law.
- The service providers may be authorized by the Central Government or the State Government to set up, maintain and upgrade the computerized facilities and also collect, retain appropriate service charges for providing such services at such scale as may be specified by the Central Government or the State Government.
- The Bill seeks to achieve the above objects.

10.1 THE IT ACT 2000 AND IT'S OBJECTIVES

This is 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 and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Objectives of the Act are:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law.
- To facilitate electronic filing of documents with Government departments
- To facilitate electronic storage of data
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions
- To give legal recognition for keeping of books of accounts by banker's in electronic form.
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

10.2 PRELIMINARY [CHAPTER I]

It contains one section and two subsections. In subsection I, Short Title, Extent, Commencement and Application are given, and in subsection II, various definitions are discussed.

10.2.1 Short Title, Extent, Commencement and Application

(1) This Act may be called the Information Technology Act, 2000. [As Amended by Information technology (Amendment) Act 2008]

P.S: Information Technology (Amendment) Bill 2006 was amended by Information Technology Act Amendment Bill 2008 and in the process, the underlying Act was renamed as Information Technology (Amendment) Act 2008 herein after referred to as **ITAA 2008**.

(2) 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.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a

reference to the commencement of that provision.[Act notified with effect from October 17, 2000. Amendments vide ITAA-2008 notified with effect from....]

(4) (Substituted Vide ITAA-2008)

Nothing in this Act shall apply to documents or transactions specified in the First Schedule by way of addition or deletion of entries thereto.

(5) (Inserted vide ITAA-2008)

Every notification issued under sub-section (4) shall be laid before each House of Parliament

10.2.2 Definitions

(1) In this Act, unless the context otherwise requires,

(a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "Adjudicating Officer" means adjudicating officer appointed under subsection (1) of section 46;

(d) "Affixing **Electronic** Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;

(e) "Appropriate Government" means as respects any matter.

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(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;

(g) "Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

(h) "Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

(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. (Inserted Vide ITAA 2008)

(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) **(Substituted vide ITAA-2008)**

"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;

(k) "Computer Resource" means computer, communication device, computer system, computer network, data, computer database 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;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Appellate * Tribunal established under sub-section (1) of section 48 (* "Regulations" omitted)

(na) (Inserted vide IT AA-2008)

"Cyber Café" 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.

(nb) (Inserted Vide ITAA 2008)

"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.

(o) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized 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;

(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;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means official Gazette published in the electronic form;

(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;

(ta) **(Inserted vide ITAA-2006)**

"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

(tb) **(Inserted vide ITAA-2006)**

"Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"

(u) "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) "Indian Computer Emergency Response Team" means an agency established under sub-section (1) of section 70 B

(v) "Information" includes data, **message**, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Amended vide ITAA-2008)

(w) **(Substituted vide ITAA-2008)**

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.-

(x) "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made there under

(z) "License" means a license granted to a Certifying Authority under section 24;

(za) Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) Prescribed" means prescribed by rules made under this Act;

(zc) Private Key" means the key of a key pair used to create a digital signature;

(zd) Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(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;

(zf) "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued;

(zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

10.3 DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (AMENDED VIDE ITAA 2008) [CHAPTER-II]

This chapter gives legal recognition to electronic records and digital signatures. It contains only **section 3**. The section provides the conditions subject to which an electronic record may

be authenticated by means of affixing digital signature. The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by any body who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message. In ITAA 2008, this section is given as follows:

[Section 3] Authentication of Electronic Records:

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

[Section 3A] Electronic Signature (Inserted vide ITAA 2006):

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-

(a) is considered reliable ; and

(b) may be specified in the Second Schedule

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament

10.4 ELECTRONIC GOVERNANCE [CHAPTER III]

This chapter is one of the most important chapters. It specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt. This chapter contains sections 4 to 10.

Section 4 provides for *"legal recognition of electronic records"*. It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form. This section is as follows:

[Section 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

Section 5 provides for *legal recognition of Digital Signatures*. Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then

such requirement shall be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

For the purposes of this section, *"signed",* with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly. This section is as follows:

[Section 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.

Explanation -

For the purposes of this section, "Signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "Signature" shall be construed accordingly.

Section 6 lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any licence or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection. This section is given as under as per ITAA 2008:

***[Section 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.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

[Section 6A] Delivery of Services by Service Provider (Inserted vide ITAA-2008):

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation: For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

Section 7 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

(i) The information therein remains accessible so as to be usable subsequently.

(ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.

(iii) The details which will facilitate the identification of the origin, destination, dates and time of despatch or receipt of such electronic record are available therein.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. ITAA 2008, this section is given as follows:

[Section 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:

However,

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.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules. regulation, etc.. in Electronic Gazette.

[Section 7A] Audit of Documents etc in Electronic form:

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form (ITAA 2008, Standing Committee Recommendation)

Section 8 provides for the publication of rules, regulations and notifications in the Electronic Gazette. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

[Section 8] Publication of rules, regulation, etc, in Electronic Gazette:

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to

have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

However

where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

However, **section 9** of the Act provides that the conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central Government or the State Government.

[Section 9] Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form:

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

[Section 10] Power to make rules by Central Government in respect of Electronic Signature (Modified Vide ITAA 2008:)

The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

10A : Validity of contracts formed through electronic means (Inserted by ITAA 2008)

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.

10.5 ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS [CHAPTER IV]

Chapter IV of the Act deals with attribution, receipt and dispatch of electronic records. 'Attribution' means 'to consider it to be written or made by someone'. Hence, this section lays down how an electronic record is to be attributed to the person who originated it. This is given in section 11. As per ITAA 2008, Section 11 is as follows:

10.14 Information Systems Control and Audit

[Section 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.

Section12 provides for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made. As per ITAA 2008, Section 12 is given as under:

[Section 12] Acknowledgement of Receipt (Modified by ITAA 2008):

(1) Where the originator has not 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.

Section 13 provides for *the manner in which the time and place of despatch and receipt of electronic record* sent by the originator shall be identified. It is provided that in general, an electronic record is deemed to be despatched at the place where the originator has his place of business and received where the addressee has his place of business.As per ITAA 2008, Section 13 is as follows:

[Section 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.

10.6 SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES [CHAPTER V]

Chapter V sets out the conditions that would apply to qualify electronic records and digital signatures as being secure. It contains sections 14 to 16.

Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. In ITAA 2008, Section 14 is given as follows:

[Section 14] Secure Electronic Record:

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

10.16 Information Systems Control and Audit

Section 15 provides for the *security procedure to be applied to Digital Signatures* for being treated as a secure digital signature. In ITAA 2008, Section 15 is given as under:

[Section 15] Secure Electronic Signature (Substituted vide ITAA 2008):

An electronic signature shall be deemed to be a secure electronic signature if-

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed

Explanation- In case of digital signature, the "signature creation data" means the private key of the subscriber

Section 16 provides for the power of the Central Government to prescribe the *security procedure* in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc. As per ITAA 2008, Section 16 is given as follows:

[Section 16] Security procedures and Practices (Amended vide ITAA 2008):

The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

10.7 REGULATION OF CERTIFYING AUTHORITIES (CHAPTER VI)

Chapter VI contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities. It contains sections 17 to 34.

Section 17 provides for the *appointment of Controller and other officers* to regulate the Certifying Authorities. As per ITAA 2008, Section 17 is given as follows:

[Section 17] Appointment of Controller and other officers (Amended Vide ITAA 2008):

(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.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees (Inserted vide ITAA 2008) shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

Section 18 lays down the *functions which the Controller may perform* in respect of activities of Certifying Authorities. As per ITAA 2008, Section 18 is given as under:

[Section 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.

Section 19 provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

[Section 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.

Section 20 : (Omitted vide ITA 2008)

Section 21 provides that a licence to be issued to a Certifying Authority to issue *Digital Signature Certificates* by the Controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the licence or reject the application after giving reasonable opportunity of being heard. As per ITAA 2008, Section 21 is given as under:

[Section 21] License to issue electronic signature certificates:

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a license to issue Electronic Signature Certificates.

(2) No license shall be issued under sub-section (1), unless the applicant fulfills 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.

(3) 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.

Section 22provides that the *application for licence* shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant. It shall be further accompanied by a fee not exceeding Rs.25,000 and other documents as may be prescribed by the Central Government. In ITAA 2008, section 22 is given as follows:

[Section 22] Application for license:

(1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a license shall be accompanied by-

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

Section 23 provides that the application for *renewal of a licence* shall be in such form and accompanied by such fees not exceeding Rs.5,000 which may be prescribed by the Central Government. In ITAA 2008, Section 23 is given as follows:

[Section 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:

Section 24 deals with the procedure for *grant or rejection of licence* by the controller on certain grounds. No application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case. In ITAA 2008, Section 24 is given as follows:

[Section 24] Procedure for grant or rejection of license:

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

However,

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

Section 25 provides that the Controller may *revoke a licence* on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

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

Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Thereafter, the Controller shall publish a notice of suspension or revocation of license as the case may be in the database maintained by him.

Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock. It is also provided that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate. As per ITAA 2008, different sections are given as follows:

[Section 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 specified in Section 30 [Substituted for the words "under clause (b) of sub-section (2) of section 20;" vide amendment dated September 19, 2002]

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

However,

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

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him:

However,

no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

[Section 26] Notice of suspension or revocation of license:

(1) 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.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

However,

the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock

However,

that the Controller may, if he considers necessary, publicize the contents of the data-base in such electronic or other media, as he may consider appropriate.

[Section 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.

The Controller or any person authorised by him, shall have access to any computer system, data or any other material connected with such system if he has reasonable cause to suspect that contravention of the provisions of the Act or the rules or regulation is being committed.

[Section 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.

[Section 29] Access to computers and data:

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(Amended vide ITAA 2008)

(2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.

[Section 30] Duties of Certifying Authorities:

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:

Every Certifying Authority shall-

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse:

(b) provide a reasonable level of reliability in its services which arc reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (**Amended vide ITAA 2008)**

(ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and **(Inserted vide ITAA 2008)**

(d) observe such other standards as may be specified by regulations.

[Section 31] Certifying Authority to ensure compliance of the Act, etc.:

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

[Section 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.

[Section 33] Surrender of license:

(1) Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.

(2) Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offense and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

[Section 34] Disclosure:

(1) Every Certifying Authority shall disclose in the manner specified by regulations

(a) its Electronic Signature Certificate (Amended vide ITAA 2008)

(b) any certification practice statement relevant thereto;

(c) notice of revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall-

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

10.8 ELECTRONIC SIGNATURE CERTIFICATES [CHAPTER VII]

Chapter VII of the Act contains Sections 35 to 40.

Section 35 lays down the procedure for issuance of a Digital Signature Certificate. It provides that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000. The fee shall be prescribed by the Central Government, and different fees may be prescribed for different classes of applicants.

The section also provides that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that –

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) 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 applicant.

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

(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:

However,

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

However,

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

10.24 Information Systems Control and Audit

Section 36 required that while issuing a Digital Signature Certificate, the Certifying Authority should certify that it has complied with the provisions of the Act, the rules and regulations made there under and also with other conditions mentioned in the Digital Signature Certificate.

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 (Inserted vide ITAA 2008)

(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 (Inserted vide ITAA 2008)

(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).

[Section 37] Suspension of Digital Signature Certificate:

The Certifying Authority may suspend such certificate if it is of the opinion that such a step needs to be taken in public interest.

Such certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard.

Suspension of Digital Signature Certificate

Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate -

(a) on receipt of a request to that effect from -

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorized to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Section 38 provides for the *revocation of Digital Signature Certificates* under certain circumstances. Such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. Upon revocation or suspension the certifying Authority shall publish the notice of suspension or revocation of a Digital Signature Certificate.

Revocation of Digital Signature Certificate

A Certifying Authority may revoke a Digital Signature Certificate issued by it

(a) where the subscriber or any other person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that -

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

[Section 39] Notice of suspension or revocation:

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

10.9 DUTIES OF SUBSCRIBERS [CHAPTER VIII]

This Chapter contains **sections 40 to 42**. It specifies duties of subscribers. As per ITAA 2008, different Sections are as under:

[Section 40] Generating Key Pair:

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, (*) the subscriber shall generate that [substituted for "the" vide amendment dated 19/09/2002] key pair by applying the security procedure. [* word "then"-*deleted vide amendment dated 19/9/2002*],

[Section 40A] Duties of subscriber of Electronic Signature Certificate:

In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed. (Inserted Vide ITAA 2008)

[Section 41] Acceptance of Digital Signature Certificate:

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate -

  (a) to one or more persons;

  (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

  (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

  (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

  (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

[Section 42] Control of Private key:

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the r public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.["to a person not authorized to affix the digital signature of the subscriber".-Omitted vide amendment dated 19/09/2002]

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation - For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate—

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature

(c) Certificate in any manner.

By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

10.10 PENALTIES AND ADJUDICATION [CHAPTER IX]

Chapter IX contains sections 43 to 47. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudication Officer for holding an inquiry in relation to certain computer crimes and for awarding compensation. Sections 43 to 45 deal with different nature of penalties.

Section 43 deals with penalty for damage to computer, computer system, etc by any of the following methods:

[Section 43] Penalty and Compensation for damage to computer, computer system, etc. (Amended vide ITAA-2008):

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

(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)

(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 authorized 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 there under,

(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 **(Inserted vide ITAA-2008)**

(j) 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, (Inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation to the person so affected. (change vide ITAA 2008)

Explanation - for the purposes of this section -

(i) "Computer Contaminant" means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

Compensation for failure to protect data (Inserted vide ITAA 2006)

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, to the person so affected. (Change vide ITAA 2008)

Explanation: For the purposes of this section

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[Section 44] Penalty for failure to furnish information, return, etc.:

If any person who is required under this Act or any rules or regulations made there under 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.

Section 45 provides for 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. As per ITAA 2008, Section 45 is given as under:

[Section 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.

Section 46 confers the *power to adjudicate contravention* under the Act to an officer not below than the rank of a Director to the Government of India or an equivalent officer of a State Government. Such appointment shall be made by the Central Government. In order to be eligible for appointment as an adjudicating officer, a person must possess adequate experience in the field of Information Technology and such legal or judicial experience as may be prescribed by the Central Government. The adjudicating officer so appointed shall be responsible for holding an inquiry in the prescribed manner after giving reasonable opportunity of being heard and thereafter, imposing penalty where required. In ITAA 2008, section 46 is given as follows:

[Section 46] Power to Adjudicate:

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government. **(amended vide ITAA 2008)**

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crores.

Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees five crores shall vest with the competent court. (Inserted Vide ITAA 2008).

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and -

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

(c) shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908 (Inserted vide ITAA 2008)

Section 47 provides that while deciding upon the quantum of compensation, the adjudicating officer shall have due regard to the amount of gain of unfair advantage and the amount of loss caused to any person as well as the respective nature of the default. As per ITAA 2008, Section 47 is given as under:

[Section 47] Factors to be taken into account by the adjudicating officer:

While adjudging the quantum of compensation under this Chapter the adjudicating officer shall have due regard to the following factors, namely -

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default

10.11 THE CYBER APPELLATE TRIBUNAL (Amended vide ITA-2008) [Chapter X]

The "Cyber Regulations Appellate Tribunal" has appellate powers in respect of orders passed by any adjudicating officer. Civil courts have been barred from entertaining any suit or proceeding in respect of any matter which an adjudicating officer or Tribunal is empowered to handle.

Section 48 provides for establishment of one or more Appellate Tribunals to be known as Cyber Regulations Appellate Tribunals.

The Cyber Regulations Appellate Tribunal shall consist of one person only (called the Presiding Officer of the Tribunal) who shall be appointed by notification by the Central Government. Such a person must be qualified to be a judge of a High Court or is or has been a member of the Indian Legal Service in the post in Grade I of that service for at least three years.

The Presiding Officer shall hold office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier. As per ITAA 2008 different sections are given as follows:

[Section 48] Establishment of Cyber Appellate Tribunal:

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

[Section 49] Composition of Cyber Appellate Tribunal (Substituted vide ITAA 2008):

(1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint (Inserted vide ITAA-2008).

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted Vide ITAA 2008).

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. (Inserted vide ITAA-2008).

(3) Subject to the provisions of this Act-

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.

Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 (ITAA 2008)

(c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(Inserted vide ITAA-2008).

(4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench (Inserted vide ITAA-2008)

(5) If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. (Inserted vide ITAA-2008)

[Section 50] Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal (Substituted vide ITAA 2006):

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court; (substituted vide ITAA-2008)

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the central Government or State Government for a period of not less than seven years.

(Inserted vide ITAA-2008)

(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that service for a period of not less than five years.

[Section 51] Term of office, conditions of service etc of Chairperson and Members (Substituted vide ITAA 2008):

(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier. (Inserted vide ITAA 2008)

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member. (Inserted vide ITAA 2008)

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member. (Inserted vide ITAA 2008).

Section 52 provides for the salary and allowances and other terms and conditions of service of the presiding Officer.

[Section 52] Salary, allowance and other terms and conditions of service of Chairperson and Member (Substituted vide ITAA 2008):

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed: (Inserted vide ITAA 2008)

[Section 52A] Powers of superintendence, direction, etc (Inserted vide ITAA 2008):

The Chairperson of he Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

[Section 52B] Distribution of Business among Benches (Inserted vide ITAA 2008):

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

[Section 52C] Powers of the Chairperson to transfer cases (Inserted vide ITAA 2008):

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

[Section 52D] Decision by majority (Inserted vide ITAA 2008):

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

Section 53 provides that in the situation of any vacancy occurring in the office of the Presiding officer of Cyber Regulations Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act.

[Section 53] Filling up of vacancies (Amended vide ITAA 2008):

If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

[Section 54] Resignation and removal (Amended vide ITAA 2008):

(1) The Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

However,

the said Chairperson or Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Chairperson or Member of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Chairperson or Member concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Chairperson or Member.

[Section 55] Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings (Inserted vide ITAA 2008):

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

[Section 56] Staff of the Cyber Appellate Tribunal (Error in amendment...item 28):

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as the Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

[Section 57] Appeal to Cyber Regulations Appellate Tribunal:

(1) Save as provided in sub-section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

However,

the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

[Section 58] Procedure and Powers of the Cyber Appellate Tribunal:

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte

(g) any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed .to be a judicial proceeding within the meaning of sections 193 arid 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

[Section 59]: Right to legal representation:

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal Limitation.

[Section 60] Limitation:

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

[Section 61] Civil court not to have jurisdiction (Amended vide ITAA 2008):

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction

shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter. (Inserted vide ITAA 2006).

[Section 62] Appeal to High court:

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

However,

the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

Compounding of contravention

Section 63 provides that any contravention under the Act may be compounded by the Controller or adjudication officer, either before or after the institution of the adjudication proceedings subject to such conditions as he may impose.

It is also provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded. However, these provisions shall not apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention committed by him, was compounded.

[Section 63] Compounding of Contravention:

(1) Any contravention under this Act [substituted for "Chapter" vide amendment dated 19/09/2002] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

However,

such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on

which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

Recovery of Penalty

Section 64 provides for recovery of penalty as arrears of land revenue and for suspension of the license or Digital Signature Certificate till the penalty is paid.

[Section 64] Recovery of Penalty or compensation (Amended vide ITAA 2006):

A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

10.12 OFFENCES [CHAPTER XI]

Chapter XI deals with some computer crimes and provides for penalties for these offences. It contains sections 65 to 78.

Section 65 provides for punishment up to three years or with a fine which may extend to Rs. 2 lakhs or with both whoever knowingly or intentionally tampers with the computer code source documents.

"Computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. As per ITAA 2008, Section 65 is given as follows:

[Section 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.

Hacking with computer system

'Hacking' is a term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the public or that person. Section 66 provides that a person who commits hacking shall be

punished with a fine upto Rs.2 lakhs or with imprisonment upto 3 years, or with both. As per ITAA 2008, Section 66 is given as follows:

[Section 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.

[Section 66 A] Punishment for sending offensive messages through communication service, etc.(Introduced vide ITAA 2008):

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 ~~t~~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.

[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008):

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.

[Section 66C] Punishment for identity theft. (Inserted Vide ITA 2008):

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.

[Section 66D] Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008):

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.

[Section 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.

[Section 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 authorization 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'.

Publishing of information which is obscene in electronic form

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs. As per ITAA 2008, Section 67 is given as under:

[Section 67] Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008):

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.

[Section 67 A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008):

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.

[Section 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.

[Section 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.

Section 68 provides that the controller may give directions to a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, so as to ensure compliance with this law. If any person fails to comply, he shall be liable to imprisonment upto 3 years or fine upto Rs.2 lakhs, or both. As per ITAA 2008, Section 68 is given as under:

[Section 68] Power of Controller to give directions (Amended Vide ITAA 2008):

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who **intentionally or knowingly** (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

Section 69 empowers the Controller, it he is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, security of the State, friendly relation with foreign states or public order, to intercept any information transmitted through any computer system or computer network. As per ITAA 2008, Section 69 is given as follows:

[Section 69] Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008):

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if ~~is~~ satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -

(a) provide access to **or secure access to** the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, **as the case may be;** or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

[***Section 69 A] Power to issue directions for blocking for public access of any information through any computer resource:***

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

[Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

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

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Section 70 empowers the appropriate Government to declare by notification any computer, computer system or computer network to be a protected system. Any unauthorized access of such systems will be punishable with imprisonment which may extend to ten years or with fine. As per ITAA 2008, Section 70 is given as under:

[Section 70] Protected system (Amended Vide ITAA-2008):

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. (Substituted vide ITAA-2008)

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system. (Inserted vide ITAA 2008)

[Section 70 A] National nodal agency. (Inserted vide ITAA 2008):

(1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

[Section 70 B] Indian Computer Emergency Response Team to serve as national agency for incident response:

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

  (a) collection, analysis and dissemination of information on cyber incidents

  (b) forecast and alerts of cyber security incidents

  (c) emergency measures for handling cyber security incidents

  (d) coordination of cyber incidents response activities

  (e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

  (f) such other functions relating to cyber security as may be prescribed

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1)

Section 71 provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both. As per ITAA 2008, Section 71 is given as follows:

[Section 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.

Section 72 provides a punishment for breach of confidentiality and privacy of electronic records, books, information, etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both. As per ITAA 2008, Section 72 is given as under:

[Section 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.

[Section 72 A] Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008):

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.

Section 73 provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both. As per ITAA 2008, Section 73 is given as follows:

[Section 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.

Section 74 provides for punishment with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both to a person whoever knowingly publishes for fraudulent purpose any Digital Signature Certificate. As per ITAA 2008, Section 74 is given as follows:

[Section 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

Section 75 provides for punishment for commission of any offence or contravention by a person outside India irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. As per ITAA 2008, Section 75 is given as follows:

[Section 75] Act to apply for offence or contraventions committed outside India:

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 76 provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules, regulations or orders made there under.

It is also provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening the provisions of this Act, rules, orders or regulations made there under as it may think fit. Section 76 is as under:

[Section 76] Confiscation:

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

However,

where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Section 77 further provides that penalty and confiscation provided under this Act shall not interfere with other punishments provided under any other law for the time being in force. Different parts of Section 77 is as follows:

[Section 77] Compensation, penalties or confiscation not to interfere with other punishment. (Substituted Vide ITAA-2008):

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. Different subsections of the section is given as follows:

[Section 77 A] Compounding of Offences:

(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

[Section 77 B] Offences with three years imprisonment to be cognizable:

Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be boilable.

Section 78 provides for power to investigate the offences under the Act by a police officer not below the rank of Deputy Superintendent of Police. This is as follows:

[Section 78] Power to investigate offences *(Amended Vide ITAA 2008):*

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act. (Amended Vide ITAA 2008)

10.13 INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES (SUBSTITUTED VIDE ITA-2006) [CHAPTER XII]

Chapter XII contains **section 79** which provides that the Network Service Providers shall be liable for any third party information or data made available by him if he proves that the offence was committed without his knowledge or consent.

Explanation – For the purposes of this section,-

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary; Section 79 is as follows:

[Section 79] Exemption from liability of intermediary in certain cases:

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. (corrected vide ITAA 2008)

(2) The provisions of sub-section (1) shall apply if-

  (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

  (b) the intermediary does not-

    (i) initiate the transmission,

    (ii) select the receiver of the transmission, and

    (iii) select or modify the information contained in the transmission

  (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)

(3) The provisions of sub-section (1) shall not apply if–

  (a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)

  (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation: For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

Examiner of Electronic Evidence (Inserted Vide ITA-2006) (CHAPTER XII A)

[Section 79A] Central Government to notify Examiner of Electronic Evidence:

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation:- For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

10.14 MISCELLANEOUS [CHAPTER XIII]

Some miscellaneous sections are as under:

[Section 80] Power of Police Officer and Other Officers to Enter, Search, etc.:

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a **Inspector** or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

Explanation

For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section

[Section 81] Act to have Overriding effect:

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 (Inserted Vide ITAA 2008)

[Section 81-A]: Application of the Act to Electronic cheque and Truncated cheque-* (Inserted vide Negotiable Instruments Amendment Act 2002, - Effective from 6th Day of February 2003):

(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and

amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

Explanation: For the purpose of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act 1881 (26 of 1881).

[Section 82]: Chairperson, Members, Officers and Employees to be Public Servants (Amended Vide ITA-2008):

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be Public Servants within the meaning of section 21 of the Indian Penal Code.

[Section 83] Power to Give Direction:

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made there under.

[Section 84] Protection of Action taken in Good Faith:

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

[Section 84 A] Modes or methods for encryption (Inserted Vide ITA-2008):

The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption

[Section 84 B] Punishment for abetment of offences (Inserted Vide ITA-2008):

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

[Section 84 C] Punishment for attempt to commit offences (Inserted Vide ITA-2008):

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

[Section 85] Offences by Companies:

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

However,

Nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation-

For the purposes of this section

(i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and

(ii) "Director", in relation to a firm, means a partner in the firm

[Section 86] Removal of Difficulties:

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

However,

no order shall be made under this section after the expiry of a period of two years from the commencement of this Act. (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

[Section 87] Power of Central Government to make rules:

(1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely

(a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A (Substituted vide ITA-2008)

(aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) f section 3A(Inserted Vide ITA-2006) (Inserted vide ITAA-2008)

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5.(Inserted vide ITAA-2008)

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed or issued and the method of payment under sub-section (2) of section 6;

(ca) the manner in which the authorized service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A (Inserted vide ITAA-2008)

(d) the matters relating to the type of Electronic Signature, manner and format in which it may be affixed under section 10;

(e) the manner of storing and affixing electronic signature creation data under section 15 (substituted vide ITAA-2008)

(ea) the security procedures and practices under section 16 (Inserted vide ITAA-2008)

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers, other officers and employees under section 17; (ITAA 2008)

(g) (omitted vide ITAA-2008)

(h) the requirements which an applicant must fulfill under sub-section (2) of section 21;

(i) the period of validity of license granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for license may be made under subsection (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(l) such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a license and the fee payable thereof under section 23;

(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35.(Inserted vide ITAA-2008)

(n) the amount of late fee payable under the proviso to section 23;

(o) the form in which application for issue of a Electronic Signature Certificate may be made under sub-section (1) of section 35;

(oa) the duties of subscribers under section 40A (Inserted vide ITAA-2008)

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A (Inserted vide ITAA-2008)

(p) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

(q) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;

(r) the qualification and experience which the adjudicating officer shall possess under sub-section (2) of section 46; (Ed: error in the act item number (vii). Bill mentions correction not in the original section-"Presiding Officer" to be replaced with "Chairman and Members")

(s) the salary, allowances and the other terms and conditions of service of the Chairman and Members under section 52; (amended vide ITAA-2008)

(t) the procedure for investigation of misbehaviour or incapacity of the Chairman and Members under sub-section (3) of section 54; (Ed: Error: bill mentions corrections to (r) and (s) instead of (s) and (t)

(u) the salary and allowances and other conditions, of service of other officers and employees under sub-section (3) of section 56;

(v) the form in which appeal may be filed and the fee thereof under subsection (3) of section 57;

(w) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52 A (substituted vide ITAA-2008)

(wa) the information, duration, manner and form of such information to be retained and preserved under section 67 C (ITAA 2008)

(x) The Procedures and safeguards for interception, monitoring or decryption under sub-section (2) of section 69 (ITAA 2008)

(xa) the procedure and safeguards for blocking for access by the public under sub-section (2) of section 69 A. (ITAA 2008)

(xb) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of section 69 B (ITAA 2008)

(y) the information security practices and procedures for protected system under section 70 (Inserted vide ITAA-2008)

(ya) manner of performing functions and duties of the agency under sub-section (3) of section 70 A (ITAA 2008)

(yb) the officers and employees under sub-section (2) of section 70 (B) (ITAA 2008)

(yc) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70 B (ITAA 2008)

(yd) the manner in which the functions and duties of agency shall be performed under sub-section (5) of section 70 B (ITAA 2008)

(z) the guidelines to be observed by the intermediaries under sub section ~~(4)~~ (2) of section 79 (Inserted vide ITAA-2008)

(za) the modes or methods for encryption under section 84A (Inserted vide ITAA-2008).

(3) Every notification made by the Central Government under sub-section (1) of section 70 (A) and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation. (ITAA 2008).

[Section 88] Constitution of Advisory Committee:

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise –

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act

(4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

[Section 89] Power of Controller to make Regulations:

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made there under to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (n) [Substituted for (m) vide amendment dated 19/09/2002] of section 18;

(b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority under sub-section (1) of section 19;

(c) the terms and conditions subject to which a license may be granted under clause (c) of sub-section (3) of section 21;

(d) other standards to be observed by a Certifying. Authority under clause (d) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35

(g) the manner by which a subscriber communicates the compromise of private key to the Certifying Authority under sub-section (2) of section 42.

(3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive- sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall there after have effect only in such modified form or be of no effect, as the ease may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

[Section 90] Power of State Government to make rules:

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely –

  (a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;

  (b) for matters specified in sub-section (2) of section 6;

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

Sections 91, 92, 93, 94 are omitted vide ITAA, 2006.

Self -examination questions

1. What are the major objectives of enacting the Information Technology Act, 2000?
2. What all are included in the definition of computer network, computer system, and data under the Act?
3. What is a secure system under Information Technology Act, 2000? Has the act suggested any technical standards for a system to be recognized as a secured system?
4. What is a digital signature? What are the attributes of a digital signature and explain that how is a document authenticated through a digital signature?
5. Explain, in short, how does enactment of Information Technology Act, 2000 paves the way for electronic governance in India?
6. What are the duties of a subscriber of a digital signature?
7. What are the major penal provisions under Information technology Act, 2000?
8. What are the powers of Cyber Appellate Tribunal? When can one make an appeal to the tribunal?
9. What are the powers of a Police Officer under the Information Technology Act to enter and search a public place?
10. What are the liabilities of companies under section 85 of the Information Technology Act?
11. Discuss the major differences between original IT Act 2000 and ITAA 2008?

Sources:

1. *www.legalserviceindia.com/cyber/itact.html*
2. *www.nicca.nic.in/pdf/itact2000.pdf*
3. *www.eprocurement.gov.in/news/actzeromod.pdf*
4. *www.naavi.org/ita-2006/index.html.*