FUTURE VISION BIE

One Stop for All Study Materials

& Lab Programs

Future Vision

By K B Hemanth Raj

Scan the QR Code to Visit the Web Page

Or

Visit : https://hemanthrajhemu.github.io

Gain Access to All Study Materials according to VTU,
CSE – Computer Science Engineering,
ISE – Information Science Engineering,
ECE - Electronics and Communication Engineering
& MORE...

Join Telegram to get Instant Updates: https://bit.ly/VTU_TELEGRAM

Contact: MAIL: futurevisionbie@gmail.com

INSTAGRAM: www.instagram.com/hemanthraj_hemu/

INSTAGRAM: www.instagram.com/futurevisionbie/

WHATSAPP SHARE: https://bit.ly/FVBIESHARE

Chapter 27

The Information Technology Act, 2000

In the contemporary digital era, electronic communication provides a cheaper, easy to operate and retrieve, and faster processing of transactions. The Information Technology (IT) Act, 2000, is an important legislation in this behalf that seeks 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' or E-Commerce. It involves use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents, with the agencies concerned. IT Act allows unrestricted monitoring of all electronic communication, even for non-cognizable offences. This Act aims to provide the legal infrastructure for e-commerce in India. Though, India lacks a full fledged ICT framework for implementation of e-governance, yet IT Act *per se* is playing an important role to facilitate e-governance by giving legal recognition to and promoting online filing of income-tax returns, corporate returns etc. The Act extends to the whole of India and it also applies to any offence or contravention thereunder committed outside India by any person. The Government of India has brought major amendments to the Information Technology Act, 2000, in the form of the Information Technology Amendment Act, 2008. The new version of the IT Act has provided additional focus on information security. It has added several new sections on offences including cyber terrorism and data protection. Department of Electronics and Information Technology under the Ministry of Communication and Information Technology concerns itself with administration of the IT Act, 2000, and other IT-related laws.

27.1 IT ACT: AIM AND OBJECTIVES

The Information Technology Act, 2000, is an important law relating to Indian cyber laws. It aims at promoting E-Commerce and facilitating E-Governance. The Act strives to achieve the following objectives:

1. To give legal recognition to transactions done by electronic way or by use of the internet.
2. To grant legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling documents online.
4. To authorise any undertaking to store their data in electronic storage.
5. To prevent cyber crime by imposing high penalty for such crimes and protect privacy of internet users.

6. To give legal recognition for keeping books of account by bankers and other undertakings in electronic form.

27.2 SCOPE OF THE ACT

The Act attempts to address the following issues:

1. Legal recognition of electronic documents
2. Legal recognition of digital signatures
3. Offences and contraventions
4. Justice dispensation systems for cybercrimes

As per Section 1(4), provisions of this Act shall not apply to the following documents or transactions:

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

27.3 MAJOR CONCEPTS

Some of the important terms used in the Information Technology Act are briefly introduced below.

Access implies gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

Addressee is a person who is intended by the originator to receive the electronic record but does not include any intermediary.

Adjudicating Officer means an adjudicating officer appointed under Section 46(1).

Affixing Digital signature means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

Appropriate Government means any matter

1. Enumerated in List II of the Seventh Schedule to the Constitution;
2. 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.

Asymmetric Crypto System is 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.

Certifying Authority is a person who has been granted a licence to issue a Digital Signature Certificate under Section 24.

Certification Practice Statement is a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates.

Computer refers to 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.

Computer Network implies the interconnection of one or more computers through—

1. The use of satellite, microwave, terrestrial line or other communication media; and
2. Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

Computer Resource refers to a computer, computer system, computer network, data, computer data base or software.

Computer system refers to 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.

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

Digital Signature refers to the authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with Section 3.

Electronic Form with reference to information refers to any information generated, sent, received, or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

Electronic Gazette refers to the Official Gazette published in the electronic form.

Electronic Record refers to any data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

Information includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche.

Intermediary, with respect to any particular electronic message, is any person who, on behalf of another person, receives, stores, or transmits that message or provides any service with respect to that message.

Key Pair, in an asymmetric crypto system, implies 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.

Originator refers to 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.

Private Key refers to the key of a key pair used to create a digital signature.

Public Key refers to the key of a key pair used to verify a digital signature, which is listed in the Digital Signature Certificate.

Secure System refers to computer hardware, software, and procedure that
1. is reasonably secure from unauthorised access and misuse;
2. provides a reasonable level of reliability and correct operation;
3. is reasonably suited to performing the intended functions; and
4. adheres to generally accepted security procedures;

27.4 IMPORTANT PROVISIONS

Important provisions of the Act have been briefly explained below.

27.4.1 Digital Signature: Authentication of Electronic Records

A digital signature is basically a way to ensure that an electronic record or document (e- mail, spreadsheet, text file, etc.) is authentic. The Act contains the following provisions in relation to digital signature:

1. 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 the 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 3].

27.4.2 Electronic Governance: Legal Recognition of Electronic Records

E-Governance is the public sector's use of information and communication technologies (ICT) with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective. The three main target groups that can be distinguished in governance concepts are government, citizens and businesses/interest groups. Generally four basic models of E-Governance are available—government-to-citizen (customer), government-to-employees, government-to-government and intergovernmental (government-to-business).

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 a law, the requirement shall be deemed to have been satisfied if such information or matter is
1. rendered or made available in an electronic form; and
2. accessible so as to be usable for a subsequent reference [Section 4].

27.4.3 Electronic Governance: Legal Recognition of Digital Signatures

A Digital Signature is the electronic or digital equivalent of a physical signature. Just as a physical signature on a paper document establishes the origin of that document, a digital signature affixed to a digital document (soft copy) establishes the origin of that digital document. Digital signatures are considered much more secure and 'fool-proof' compared to physical signatures. While, physical signatures can be easily replicated or 'forged', the technology behind digital signatures makes it virtually impossible to forge them. More specifically, in India, the IT Act provides the legal sanctity for using digital signatures.

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (then, notwithstanding anything contained in such a law, the requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of a digital signature affixed in such a manner as may be prescribed by the Central Government [Section 5].

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

27.4.4 Use of Electronic Records and Digital Signatures in Government and Its Agencies

Because of the higher security associated with digital signatures and many advantages associated with storing documents electronically (as opposed to paper), governments in many countries, including India of-course, have passed laws and regulations encouraging (and in some cases mandating) the usage of digitally signed electronic documents rather than paper documents. In India, for instance, Income-tax returns, Corporate returns etc. are to be digitally signed and uploaded electronically.

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 licence, 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 a 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 of any electronic record under clause (a) [Section 6].

27.4.5 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, if
   (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 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 [Section 7].

27.4.6 Publication of Rules and Regulations in the 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 a requirement shall be deemed to have been satisfied if such a rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matter is 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.

A person has no right to insist on accepting document in eletronic 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 9].

27.4.7 Power to Make Rules by Central Government in Respect of Digital Signature

The Central Government may prescribe

1. the type of digital signature;
2. the manner and format in which the digital signature shall be affixed;
3. the manner or procedure which facilitates identification of the person affixing the digital signature;
4. control processes and procedures to ensure adequate integrity, security, and confidentiality of electronic records or payments; and
5. any other matter which is necessary to give legal effect to digital signatures [Section 10].

27.5 ATTRIBUTION, ACKNOWLEDGMENT, AND DESPATCH OF ELECTRONIC RECORDS

27.5.1 Attribution of Electronic Records

An electronic record shall be attributed to the originator

1. if it was sent by the originator himself;
2. by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

3. by an information system programmed by or on behalf of the originator to operate automatically [Section 11].

27.5.2 Acknowledgment of Receipt

1. Where the originator has not agreed with the addressee that the acknowledgment of the receipt of the 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 originafor 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 an electronic record by him, then, unless acknowledgment has been so received, the electronic record shall be deemed to have never been 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 specify 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 12].

27.5.3 Time and Place of Dispatch and Receipt of Electronic Record

1. Unless 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. Unless 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. Unless otherwise agreed to 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 purpose of this Section,

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be termed 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, refers to the place where it is registered [Section 13].

27.6 SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

27.6.1 Secure Electronic Record

Where any security procedure has been applied to an electronic record at a specific point of time, then such a record shall be deemed to be a secure electronic record from such a point of time to the time of verification [Section 14].

27.6.2 Secure Digital Signature

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was

1. unique to the subscriber affixing it;
2. capable of identifying such a subscriber;
3. created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such a digital signature shall be deemed to be a secure digital signature [Section 15].

27.6.3 Security Procedure

The Central Government shall, for the purpose of this Act, prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including

1. the nature of the transaction;
2. the level of sophistication of the parties with reference to their technological capacity;
3. the volume of similar transactions engaged in by other parties;
4. the availability of alternatives offered to but rejected by any party;
5. the cost of alternative procedures; and
6. the procedures in general use for similar types of transactions or communications [Section 16].

27.7 REGULATION OF CERTIFYING AUTHORITIES: APPOINTMENT OF CONTROLLER AND OTHER OFFICERS

1. The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act, and may also, by the same or subsequent notification, appoint such a number of Deputy Controllers and Assistant Controllers 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 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 17].

27.7.1 Functions of the Controller

The Controller may perform all or any of the following functions, namely:

1. exercising supervision over the activities of the Certifying Authorities;
2. certifying public keys of the Certifying Authorities;
3. laying down the standards to be maintained by the Certifying Authorities;
4. specifying the qualifications and experience that which employees of the Certifying Authorities should possess;
5. specifying the conditions subject to which the Certifying Authorities shall conduct their business;
6. specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
7. specifying the form and content of a Digital Signature Certificate and the key;
8. specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
9. specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
10. facilitating the establishment of any electronic system by a Certifying Authority, either solely or jointly with other Certifying Authorities, and the regulation of such systems;
11. specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
12. resolving any conflict of interest between the Certifying Authorities and the subscribers;
13. laying down the duties of the Certifying Authorities;
14. 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 the public [Section 18].

27.7.2 Recognition of Foreign Certifying Authorities

1. The Controller may, with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
2. Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
3. The Controller, 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) may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition [Section 19].

27.7.3 Controller to Act As Repository

1. The Controller shall be the repository of all Digital Signature Certificates issued under this Act.
2. The Controller shall
   (a) make use of hardware, software, and procedures that are secure of intrusion and misuse;
   (b) observe other such standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures is assured.
3. The Controller shall maintain a computerised data base of all public keys in such a manner that such a data base and the public keys are available to any member of the public [Section 20].

27.7.4 Licence to Issue Digital Signature Certificates

Having a 'Digital Signature Certificate' (DCS) is necessary to digitally sign a document. A DSC contains what is known as a 'key-pair' comprising a private key and a corresponding public key. The private key is to be maintained securely and confidentially (i.e. in private). The public key is shared with receivers of documents In India, the Government, via the 'Controller of Certifying Authorities' has authorized a set of entities to issue DSC. The process of obtaining a DSC essentially involves submission of paperwork that establishes applicant's identity to the issuer.

1. Any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.
2. No licence 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 Digital Signature Certificates as may be prescribed by the Central Government.
3. A licence 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 21].

27.7.5 Application for Licence

1. Every application for issue of a licence shall be in such a form as may be prescribed by the Central Government.
2. Every application for issue of a licence shall be accompanied by
   (a) a certification practice statement;
   (b) a statement including the procedures with respect to the identification of the applicant;
   (c) payment of such fees, not exceeding `25000 as may be prescribed by the Central Government;
   (d) such other documents, as may be prescribed by the Central Government [Section 22].

27.7.6 Renewal of Licence

An application for renewal of a licence shall be

1. in the required form;
2. accompanied by such fees, not exceeding ₹5000, as may be prescribed by the Central Government and shall be made not less than 45 days before the date of expiry of the period of validity of the licence [Section 23].

27.7.7 Procedure for Grant or Rejection of Licence

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 licence or reject the application.

However, no application can be rejected under this Section unless the applicant has been given a reasonable opportunity of presenting his case [Section 24].

27.7.8 Suspension of Licence

1. The Controller may, if he is satisfied after making such inquiries, as he thinks fit, that a Certifying Authority has,
   - (a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
   - (b) failed to comply with the terms and conditions subject to which the licence was granted;
   - (c) failed to maintain the standards specified under clause (b) of sub-section (2) of Section 20;
   - (d) contravened any provisions of this Act, rule, regulation, or order made thereunder, revoke the licence:

     Provided that no licence 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 licence under sub-section (1), by order, suspend such a licence pending the completion of any inquiry ordered by him.

   However, no licence can 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 licence has been suspended shall issue any Digital Signature Certificate during such suspension [Section 25].

27.7.9 Notice of Suspension or Revocation of Licence

1. Where the licence 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 database maintained by him.
2. Where one or more repositories are specified, the Controller shall publish notices of such suspensions or revocations, as the case may be, in all such repositories:

   Provided that 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:

   Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media as he may consider appropriate [Section 26].

27.7.10 Power to Delegate

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller, or any officer, to exercise any of the powers of the Controller under this Chapter [Section 27].

27.7.11 Power to Investigate Contraventions

1. The Controller, or any officer authorised by him in this behalf, shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.
2. The Controller, or any officer authorised by him in this behalf, shall exercise powers like those 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 28].

27.7.12 Access to Computers and Data

1. Without prejudice to the provisions of sub-section (1) of Section 69, the Controller, or any person authorised by him, shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder 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.
2. For the purposes of sub-section (1), the Controller or any person authorised 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 assistance as he may consider necessary [Section 29].

27.7.13 Certifying Authority to Follow Certain Procedures

Every Certifying Authority shall

1. make use of hardware, software and procedures that are secure from intrusion and misuse;
2. provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
3. adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
4. observe such other standards as may be specified by regulations [Section 30].

27.7.14 Certifying Authority to Ensure Compliance of the Act

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 thereunder [Section 31].

27.7.15 Display of Licence

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business [Section 32].

27.7.16 Surrender of Licence

1. Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.
2. Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ₹10,000 or both [Section 33].

27.7.17 Disclosure

1. Every Certifying Authority shall disclose in the manner specified by regulations
   (a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
   (b) any certification practice statement relevant thereto;
   (c) notice of the 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 Digital 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 Digital 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 [Section 34].

27.8 DIGITAL SIGNATURE CERTIFICATES

Digital Signature Certificate (DSC) is a certificate, issued by a 'Certifying Authority', necessary for an undertaking to be able to digitally sign a document.

27.8.1 Certifying Authority to Issue Digital Signature Certificate

1. Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.
2. Every such application shall be accompanied by a fee not exceeding ₹25,000 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. Each 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 any other statement under sub-section.
5. and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or, for reasons to be recorded in writing, reject the application:
   Provided that no 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 [Section 35].

27.8.2 Representations upon Issuance of Digital Signature Certificate

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

1. it has complied with the provisions of this Act and the rules and regulations made thereunder;
2. it has published the Digital Signature Certificate or otherwise made it available to such a person relying on it and the subscriber has accepted it;
3. the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
4. the subscriber's public key and private key constitute a functioning key pair;
5. the information contained in the Digital Signature Certificate is accurate; and
6. 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 36].

27.8.3 Suspension of Digital Signature Certificate

1. Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such a 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 authorised to act on behalf of that subscriber,
   (b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest
2. A Digital Signature Certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity to be heard in the matter.
3. On suspension of a Digital Signature Certificate under this Section, the Certifying Authority shall communicate the same to the subscriber [Section 37].

27.8.4 Revocation of Digital Signature Certificate

1. A Certifying Authority may revoke a Digital Signature Certificate issued by it
   (a) where the subscriber, or any other person authorised by him, makes a request to that effect
   (b) upon the death of the subscriber
   (c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
2. 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 the 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, has been dissolved, wound-up or otherwise ceased to exist
3. A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity to be heard in the matter.

4. On revocation of a Digital Signature Certificate under this Section, the Certifying Authority shall communicate the same to the subscriber [Section 38].

27.8.5 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 a suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for the publication of such a notice.
2. Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspensions or revocations, as the case may be, in all such repositories [Section 39].

27.9 DUTIES OF SUBSCRIBERS

27.9.1 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 the key pair by applying the security procedure [Section 40].

27.9.2 Acceptance of Digital Signature Certificate

1. A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises 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 41].

27.9.3 Control of Private Key

1. Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
2. If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, the subscriber shall communicate this 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 until he has informed the Certifying Authority that the private key has been compromised [Section 42].

27.10 PENALTIES AND ADJUDICATION

27.10.1 Penalty for Damage to Computer, Computer System

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

1. accesses or secures access to such computer, computer system, or computer network;
2. downloads, copies or extracts any data, computer data base or information from such a computer, computer system or computer network, including information or data held or stored in any removable storage medium;
3. introduces, or causes to be introduced, any computer contaminant or computer virus into any computer, computer system, or computer network;
4. damages, or causes to be damaged, any computer, computer system or computer network, data, computer data base, or any other programme residing in such a computer, computer system or computer network;
5. disrupts, or causes disruption of, any computer, computer system or computer network;
6. denies access, or causes the denial of access, to any person authorised to access any computer, computer system or computer network by any means;
7. provides any assistance to any person to facilitate access to a computer, computer system, or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
8. 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, he shall be liable to pay damages by way of compensation not exceeding ₹1 crore to the person so affected.

Explanation: For the purpose of this Section,

1. **computer contaminant** means any set of computer instructions that are designed
   - (a) to modify, destroy, record, transmit any data or programme residing within a computer, computer system or computer network; or
   - (b) by any means usurp the normal operation of the computer, computer system, or computer network;
2. **computer data base** refers to a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that is prepared, or has been prepared, in a formalised manner, or has been produced by a computer, computer system or computer network, and is intended for use in a computer, computer system or computer network;
3. **computer virus** refers to 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;
4. **to damage** means to destroy, alter, delete, add, modify, or rearrange any computer resource by any means [Section 43].

27.10.2 Compensation for Failure to Protect Data

If 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 gain to any person, such body corporate shall be liable to pay damages to the aggrieved party [Section 43A].

27.10.3 Penalty for Failure to Furnish Information Return

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

1. 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 ₹150,000 for each such failure;
2. file any return or furnish any information, books or other documents within the time specified in the regulations, fails to file return or furnish the same within the time specified in the regulations, he shall be liable to a penalty not exceeding ₹5000 for every day during which such failure continues;
3. maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ₹10,000 for every day during which the failure continues [Section 44].

27.10.4 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 ₹25,000 to the person affected by such contravention [Section 45].

27.10.5 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 thereunder, the Central Government shall, subject to the provisions of sub-section (3), appoint an 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 to hold an enquiry in the manner prescribed by the Central Government.
2. The adjudicating officer shall, after giving the person referred to in sub-section (1) reasonable opportunity for making a representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, impose such penalty or award such compensation 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 is 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 Section 58(2), 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 [Section 46].

27.10.6 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:

1. the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
2. the amount of loss caused to any person as a result of the default;
3. the repetitive nature of the default [Section 47].

27.11 THE CYBER REGULATIONS APPELLATE TRIBUNAL

27.11.1 Establishment of Cyber Appellate Tribunal

1. The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations 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 48].

27.11.2 Composition of Cyber Appellate Tribunal

A Cyber Appellate Tribunal shall consist of one person only (hereafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government [Section 49].

27.11.3 Qualifications for Appointment As Presiding Officer of Cyber Appellate Tribunal

A person shall not qualify for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he

1. is, or has been, or is qualified to be, a Judge of a High Court; or
2. is or has been a member of the Indian Legal Service and is holding, or has held, a post in Grade I of that Service for at least three years [Section 50].

27.11.4 Term of Office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters the office, or until he attains the age of 65 years, whichever is earlier [Section 51].

27.11.5 Salary, Allowances, and Other Terms and Conditions of Service of Presiding Officer

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment [Section 52].

27.11.6 Filling Up of Vacancies

If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy. The proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled [Section 53].

27.11.7 Resignation and Removal

1. The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

   Provided that the said Presiding Officer 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 Presiding Officer of a Cyber Appellate Tribunal shall not be removed from office except by an order by the Central Government on the ground of proven misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and has been given reasonable opportunity to be 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 Presiding Officer [Section 54].

27.11.8 Orders Constituting Appellate Tribunal To Be Final

No order of the Central Government appointing any person as the Presiding Officer 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 55].

27.11.9 Staff of the Cyber Appellate Tribunal

1. The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.
2. The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under the general superintendence of the Presiding Officer.
3. The salaries, allowances and other conditions of service of the officers and employees or the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government [Section 56].

27.11.10 Appeal to Cyber Appellate Tribunal

1. Save as provided in sub-section (2), any person aggrieved by an order made by the Controller or an adjudicating officer under this Act may refer 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 25 days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved, and it shall be in such form and be accompanied by such fees as may be prescribed:

   Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of 25 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 for 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 as expeditiously as possible and endeavour shall be made by the Tribunal to dispose of the appeal finally within six months from the date of receipt of the appeal [Section 57].

27.11.11 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 its 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 pane;
   (g) any other matter which may be prescribed.
3. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228, and for the purposes of Section 196 of the Indian Penal Code. 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 58].

27.11.12 Right to Legal Representation

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal [Section 59].

27.11.13 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 60].

27.11.14 Civil Court Not to Have Jurisdiction

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 [Section 61].

27.11.15 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 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal 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 60 days [Section 62].

27.11.16 Compounding of Contraventions

1. Any contravention under this Chapter may, either before or after the institution of adjudication proceedings, be compounded by the Controller or any other such officer as may be specially authorised 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:

   Provided that such a 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 [Section 63].

27.11.17 Recovery of Penalty

A penalty imposed under this Act, if not paid, shall be recovered as an arrear of land revenue, and the licence or the Digital Signature Certificate, as the case may be, shall be suspended until the penalty is paid [Section 64].

27.12 OFFENCES

27.12.1 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 a fine which may extend up to ₹2 lakh, or with both.

Explanation: For the purposes of this section, 'computer source code' refers to the listing of programmes, computer commands, design and layout, and programme analysis of computer resource in any form [Section 65].

27.12.2 Hacking with Computer System

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 three years or with fine which may extend to five lakh rupees or with both [Section 66].

Note: In a related development, the Supreme Court on March 24, 2015 terming it unconstitutional struck down Section 66A of the IT Act which allowed arrests for posting offensive content on social media sites. The controversial provision made posting offensive material on social networking sites an offence punishable by up to three years in jail.

27.12.2 Punishment for Receiving Stolen Computer Resource or Communication Device

Whoever dishonestly received or retains any stolen computer resource of 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 66B].

27.12.3 Punishment for Identity Theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any 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 66B].

27.12.4 Punishment for Cheating by Personation by Using Computer Resource

Whoever, by means for any communication device or computer resource cheats by personating, 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 66D].

27.12.5 Punishment for Violation of Privacy

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 [Section 66E].

27.12.6 Punishment for Cyber Terrorism

1. Whoever,
   (a) With intent to threaten the unity, integrity, security of 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 authorization 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; 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 [Section 66F].

27.12.7 Publishing of Information Which Is Obscene in Electronic Form

Whoever publishes or transmits or causes to be published in the electronic form any material which is lascivious or appeals to the prurient interest, or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ₹1 lakh. In the event of a second or subsequent conviction, the punishment would be imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to ₹2 lakh [Section 67].

27.12.8 Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act in Electronic Form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for term which may extend to seven years and also with fine which may extend to ten lakh rupees [Section 67A].

27.12.9 Power of Controller to Give Directions

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 thereunder.
2. Any person who 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 three years or to a fine not exceeding ₹2 lakh, or to both [Section 68].

27.12.10 Government's Agency Power to Intercept Information

1. The Act empowers the Central/State Government's authorised agency to intercept, monitor or decrypt any information generated, transmitted, received, or stored in any computer resource if it is deemed fit in the interest of the sovereignty or integrity of India, defence 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 or for investigation of any offence.
2. The agency can also secure all the facilities and technical assistance from the subscriber or computer personnel to decrypt the information.
3. The subscriber or any person who fails to assist the agency shall be punishable with an imprisonment for a term which may extend to seven years [Section 69].

27.12.11 Protected System

1. The appropriate Government may, by notification in the Official Gazette, declare any computer, computer system, or computer network to be a protected system.

2. The appropriate Government may, by order in writing, authorise the persons who are authorised 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 10 years and shall also be liable to fine [Section 70].

27.12.12 Penalty for Misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital 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 ₹1 lakh, or with both [Section 71].

27.12.13 Penalty for 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 pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, 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 ₹1 lakh, or with both [Section 72].

27.12.14 Penalty for Publishing Digital Signature Certificate False in Certain Particulars

1. No person shall publish a Digital 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 a 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 ₹1 lakh, or with both [Section 73].

27.12.15 Publication for Fraudulent Purpose

Whoever knowingly creates, publishes, or otherwise makes available a Digital 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 ₹1 lakh, or with both [Section 74].

27.12.16 Act to Apply for Offence or Contravention 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 75].

27.12.17 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 or rules, orders or regulations made thereunder 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 any such computer, computer system, floppies, compact disks, tape drives, or any other accessories relating thereto is/are found, is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for the confiscation of such a computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto, make any other order authorised by this Act against the person contravening the provisions of this Act, rules, orders or regulations made thereunder, as it may think fit [Section 76].

27.12.18 Penalties or Confiscation Not to Interfere with Other Punishments

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force [Section 77].

27.12.19 Power to Investigate Offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act [Section 78].

27.13 NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him, if he proves that the offence or contravention was committed without his knowledge, or that he had exercised all due diligence to prevent the commission of such an offence or contravention.

Explanation: For the purposes of this Section,

- 'network service provider' means an intermediary;
- 'third party information' means any information dealt with by a network service provider in his capacity as an intermediary [Section 79].

27.14 MISCELLANEOUS PROVISIONS

27.14.1 Power of Police Officer and Other Officers to Enter, Search

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised 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 an 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 80].

27.14.2 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 [Section 81].

27.14.3 Controller, Deputy Controller, and Assistant Controllers to Be Public Servants

The Presiding Officer 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 82].

27.14.4 Power to Give Directions

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 thereunder [Section 83].

27.14.5 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 Presiding Officer, adjudicating officers, and the staff of the Cyber Appellate Tribunal, for anything which is done in good faith or is intended to be done in pursuance of this Act, or any rule, regulation or order made thereunder [Section 84].

27.14.6 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 thereunder 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 thereunder 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 a 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

(a) 'company' means any corporate body and includes a firm or other association of individuals; and

(b) 'director', in relation to a firm, refers to a partner in the firm [Section 85].

27.14.7 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:
   Provided that 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 possible after it is made, before each House of Parliament [Section 86].

27.14.8 Constitution of Advisory Committee

1. The Central Government shall, as soon as possible 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 a 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. The non-official members of such Committee shall be paid such travelling and other allowances as the Central Government may fix [Section 88].

27.14.9 Special Provisions for Evidence Relating to Electronic Record

The contents of electronic records may be proved in accordance with the provisions of Section 65B [Section 65A].

27.14.10 Admissibility of Electronic Records

Any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer (computer output) shall also be deemed to be a document, if the conditions mentioned in this Section are satisfied in relation to the information and the computer in question, and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible [Section 65B].

27.14.11 Presumption As to Electronic Records and Digital Signatures

1. In any proceedings involving a secure electronic record, the Court shall presume, unless the contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.
2. In any proceedings, involving a secure digital signature, the Court shall presume, unless the contrary is proved, that

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this Section shall create any presumption relating to the authenticity and integrity of the electronic record or any digital signature [Section 85B].

27.14.12 Presumption As to Digital Signature Certificates

The Court shall presume, unless the contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber [Section 85C].

27.14.13 Presumption As to Electronic Messages

After Section 88, the following section shall be inserted, namely:

The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation: For the purpose of this Section, the expressions 'addressee' and 'originator' shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of Section 2 of the Information Technology Act, 2000 [Section 85C].

OBJECTIVE-TYPE QUESTIONS

27.1 'Secure system' refers to computer hardware, software, and procedure that

(a) is reasonably secure from unauthorised access and misuse, and adheres to generally accepted security procedure

(b) provides a reasonable level of reliability and correct operation

(c) is reasonably suited to performing the intended functions

(d) complies with all of the above

27.2 'Subscriber' refers to

(a) a person in whose name the Digital Signature Certificate is issued

(b) any person who, on behalf of another person, receives, stores, or transmits that message or provides any service with respect to that message

(c) a person who has been granted a licence to issue a Digital Signature Certificate under Section 24

(d) None of the above

27.3 A person shall be liable to pay damages by way of compensation to the person so affected if s/he 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

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

(d) commits any of the above acts

27.4 Who, among the following, is empowered to suspend or revoke the 'licence to issue Digital Signature Certificates' granted to a Certifying Authority?

(a) Controller (b) Adjudicating officer

(c) Cyber Appellate Tribunal (d) Central Government

27.5 If the Certifying Authority fails to furnish any document, return, or report to the Controller under Section 44, it shall be liable to a penalty

(a) not exceeding ₹150,000 for each such failure

(b) not exceeding ₹5000 for every day during which such failure continues

(c) not exceeding ₹10,000 for every day during which such failure continues

(d) not exceeding ₹25,000

REVIEW QUESTIONS

27.1 Define the following terms under the Information Technology Act, 2000:

(a) Addressee (b) Certifying Authority

(c) Controller (d) Cyber Appellate Tribunal

(e) Intermediary (f) Subscriber

(g) Licence (h) Digital Signature

(i) Secure System (j) Information

27.2 What is the Information Technology Act? Discuss its aim and objectives.

27.3 Describe the provisions of the IT Act as regards the following:

(a) Legal recognition of electronic records

(b) Authentication of electronic records

(c) Retention of electronic records

(d) Publication of rules, regulations etc., in the electronic Gazette

27.4 Who is a 'Controller'? Outline his functions and powers.

27.5 Describe the duties of subscribers. Discuss also the penalties and Adjudication under Section 43 of the IT Act, 2000 for (a) damage to a computer, computers system etc., and (b) failure to furnish information, return, etc.

ANSWERS TO OBJECTIVE-TYPE QUESTIONS

27.1 (d) 27.2 (d) 27.3 (d) 27.4 (d) 27.5 (d)