The Information Technology Act, 2000

IT ACT: AIM AND OBJECTIVES :

- To give legal recognition to transactions done by electronic way or by use of the internet.
- To grant legal recognition to digital signature for accepting any agreement via computer.
- To provide facility of filling documents online.
- To authorise any undertaking to store their data in electronic storage.
- To prevent cyber crime by imposing high penalty for such crimes and protect privacy of internet users.
- To give legal recognition for keeping books of account by bankers and other undertakings in electronic form.

SCOPE OF THE ACT

SCOPE: 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 system for cybercrimes.

The Act is not applicable for following documents or transaction :-

1. A negotiable instrument as defined in the Negotiable Instruments Act, 1881.
2. A power of attorney as defined in the Power-of-Attorney Act,1882.
3. A trust as defined in the Indian Trust 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.

Major concepts

- **Access:** Gaining entry into, introduction 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 adopting 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

➔Enumerated in List II of the Seventh Schedule to the Constitution.

➔Relating to any State law enacted under List III of the Seventh Schedule to Constitution, the State Government, and in any other case, the Central Government

- **Asymmetric Crypto System:** is a system of source key pair consisting of a private key for creating a digital signature and 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 related to computer in a computer system or computer network.

- **Computer Network:** implies the interconnection of one or more computers through:

  ➔The use of satellite, microwave, terrestrial line or other communication media.

  ➔Terminals or a complex consisting of two or more interconnected computers whether or not interconnection is continuously maintained.

- **Computer Resources:** refer to a computer, computer system, computer network, data, computer database 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 function.
- **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 or stored internally in the memory of the computer.

- **Digital Signature:** refers to the authentication 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 electronic form or micro film or computer generated micro fiche.
- **Information:** includes data, text, images, sound, voice, codes, computer programs, software and database 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:** refer 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 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 is reasonably secure from unauthorised access and misuse.

➔Provides a reasonable level of liability and correct operation,

➔Is reasonably suited to performing the intended functions.

➔Adheres to generally accepted security procedure.

Important provisions

1.Digital Signature :Authentication of electronic records

- Any subscriber may authenticate any electronic record by affixing the Digital signature.
- The authentication of the electronic record shall be effected by the use of the asymmetric crypto system and hash function which envelop transform initial electronic record into another electronic record.
- Any person by the use of a public key of the subscriber can verify the electronic record.
- The private key and the public key are unique to the subscriber and constitute a functioning key pair.

2.Electronic Governance: Legal recognition of electronic recor

- E-governance is the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizens participation in the decision making process and making government more accountable, transparent and effective.
- Where any law provides that info or any other matter shall be written , typed or printed form, than not with standing anything contained in such a law.
- The requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference.

3.Electronic Governance: Legal recognition of digital signature

- A digital signature is a electronic or digital equivalent of a physical signature. A digital signature affixed to a digital document establishes the origin of that digital document.

- Digital signatures are considered to be more secure and cannot be replicated easily due to the technology behind them.

- Where any law provides that info or any other matter shall be authenticated by affixing the sign or any document shall be signed or bear the sign of any person, anything contained in such a law.

4.Use of Electronic records and Digital Signature in Government and its agencies

Because of high security associated with digital signature , govts in many countries have passed laws to encourage the use of digitally signed electronic documents.

- Where any law provides:

1. The filing of any form application or any other document with any office or body or agency owned or controlled by the appropriate government in a particular manner.
2. The issue or grant of any license , permit, sanction or approval by whatever name called in a particular manner.
3. The receipt of money in a particular manner, then not 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 as the case may be is effected by means of such electronic form.

- The govt by rules can prescribe

1. The manner and format in which such electronic records shall be filed, created or issued.
2. The manner or method of payment of any fee or charges for filling, creation or issue of any electronic record.

5.Retention of electronic records

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

1. The info contained there in remains accessible so as to be usable for a subsequent reference.
2. 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.
3. 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.

- 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.

6. Publication of rules and regulations in the electronic gazett

- 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, notification or any other matter is published in the official gazette or electronic gazette.
- Provided that where any rule, regulation, order, bye-law or any other matter is published in the official 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 electronic form.

7. **Power to make rules by central government in respect of digital signature**

The central government may prescribe

- The type of digital signature
- The manner and format in which the digital signature shall be affixed.
- The manner or procedure which facilitates identification of the person affixing the digital signature
- Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments and
- Any other matter which is necessary to give legal effect to digital signatures.

Secure Electronic Records And Secure Digital Signature

Secure Electronic Record

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

Secure Digital Signature

1. Unique to the subscriber affixing it
2. Capable of identifying such a subscriber
3. Create in a manner under the exclusive control of subscriber and is linked to electronic record relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such DS shall be deemed to be a secure DS.[sec 15]

Security Procedures

1. The nature of the transaction
2. The level of Sophistication of the parties with references to their technological capacity
3. The volume of similar transactions engaged in by other parties
4. The cost of alternative procedures
5. The availability of alternatives offered to but rejected by any party.

Regulation Of Certifying Authorities

1. Appointment of controller and other officers

1. The controller shall discharge his functions under this act subject to general control and direction of central government.
2. The deputy controller and assistant controllers shall perform the functions assigned to them by the controller under the general superintendence and control of the controller.
3. 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.
4. The Head office and Branch office of 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.

2. Functions Of The Controller

The Controller may perform following functions

- Exercising supervision over the activities of the certifying authorities
- Certifying public keys of the certifying authorities
- Laying down the standards to be maintained by the certifying authorities.

- Specifying the qualifications and experience that which employees of the certifying authorities should possess
- Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of digital signature certificate and the public key;
- Specifying the form and content of a digital signature certificate and the key
- Resolving any conflict of interest between the certifying authorities and the subscribers
- Laying down the duties of the certifying authorities

3. Recognition of Foreign Certifying Authorities

- The controller may, with 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.
- Where any certifying authority is recognised under subsection(1),the digital signature certificate issued by such certifying authority shall be valid for the purposes of this act.

4. Controller to act repository

- The controller shall be the repository of all digital signature certificate issued under this act.

- Make use of hardware, software, and procedures that are secure of intrusion and misuse
- Observe other such standards as may be prescribed by the central government to ensure that the security of the digital signature is assured.
- The controller shall maintain a computerised data base of all pubic keys in such a manner that such a data base and the public keys are available of nay member of the public

5. Licence to issue Digital Signature Certificates

- The process of obtaining a DSC essentially involves submission of paperwork that establishes applicants to the issuer.
- Any person may make an application, to the controller, for a licence to issue digital signature certificates.
- No licence shall be issued under sub section(1),unless the applicant full fills such requirement's with respect to qualification, manpower, financial resources which are necessary to issue digital signature certificates as may be prescribed by the central government
- A licence granted under this section shall
- Be valid for such period as may be prescribed by the central government
- Not be transferable.

6. Application for licence

Every application for issue of a licence shall be accompanied by

1. A certification practice statement
2. A statement including the procedure with respect to the identification of the applicant
3. Such other documents as may be prescribed by the central government

7. Renewal of Licence

An application for renewal of a licence in the required form.

8. Procedure for grant or rejection of licence

The controller may, on receipt of an application under subsection(1) of section 21,after considering the documents accompanying the application.

9. Suspension of licence

The controller may, if he is satisfied after making such inquries as he thinks fit that a certifying authority has

- Made a statement in, or in relation to, the application for the issue or renewal of licence which is incorrect or false in material particular
- Failed to maintain the standards specified under clause(b)of subsection (2)of section 20
- The controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under subsection(1).by order, suspend such a licence pending the completion of any inquiry ordered by him
- No certifying authority whose licence has been suspended shall issue any digital signature certificate during such suspension

10. Notice of suspension or revocation of licence

- 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
- 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

11. Power to delegate

- The controller may in writing, authorise the deputy controller, assistant controller, or any officers to exercise any of the power of the controller .

12. Power to investigate contraventions

- The controller, or any officer authorised by him in this behalf, shall take up for investigation any contravention of the provision of this act rules or regulations made under.

13. Access to computers and data

- 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 under has been committed have access to any computer system.

14. Certifying authority to follow certain procedures

- Make use of hardware, software and procedures that are secure from intrusion and misuse
- Observe such other standards as may be specified by regulations.

15. 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.

16. Display of Licence

- Every certifying authority shall display its Licence at a place of the permises in which it carries on its business

17. Surrender of Licence

- Every certifying authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to controller.
- Where any certifying authority fails to surrender a licence under subsection(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 fine up to 100000 or both.

18. Disclosure

- The digital certificate which contains the public key corresponding to the private key used by that Certifying authority to digitally sign digital signature certificate.
- Notice of the revocation of its certifying authority certificate

Digital signature certificates

- DSC is a certificate issued by a CA necessary for an undertaking to be able to digitally sign a document.

1. Certifying authority to issue digital signature certificate.

- Any person may make an application to the CA for issue of a DSC in such form as may be prescribed by the central Government.
- Every such application shall be accompanied by fee not exceeding 25000 as may be prescribed by the central government to be paid to the CA.
- Each such application shall be accompanied by a certification practice
- Provided that no digital certificate shall be granted unless the CA is satisfied that the applicant holds the pair keys, private key which is capable of creating a digital signature, public key used to verify a DS.

2. Representations upon issuance of digital signature certificate.

A CA while issuing a DSC shall certify that

- It has complied with the provisions of this act and the rules and regulations made .
- It has published the DSC.
- The subscriber holds the private key corresponding to the public key.
- The information contained in the DSC is accurate.

3. Suspension of digital signature certificate

May suspend such a DSC

- On receipt of a request to that effect from the subscriber or any person.
- A DSC shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity to be heard in the matter.

4. Revocation of digital signature certificate

- A CA may revoke a DSC issued by it where the subscriber or any other person authorised by him, upon the death of the subscriber, winding up of the company.
- A DSC shall not be revoked unless the subscriber has been given an opportunity to be heard in the matter.
- On revocation of a DSC under this section, the CA shall communicate the same to the subscriber.

5.Notice of suspension or revocation

- Where a DSC is suspended or revoked under sec 37 or 38, the CA shall publish a notice of such a suspension or revocation in the repository specified in the DSC for publication of such a notice.

Duties of subscribers

1. Generating key pair.

2. Acceptance of digital signature certificate:

- A subscriber shall be deemed to have accepted a DSC if he publishes the publication of a DSC to one or more persons, in a repository.
- By accepting a DSC, the subscriber certifies to all who reasonably rely on the information contained in the DSC that the subscriber holds the pair or all representations made by the subscriber to the CA.

3. Control of private key

- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his DSC and take all steps to prevent its disclosure to a person not authorised to affix the DS of the subscriber.
- If the private key corresponding to the public key listed in the DSC has been compromised, the subscriber shall communicate this without any delay to the CA in such manner as may be specified by the regulations.

Penalties and adjudication

1. Penalty for damage to computer, computer system.

- If any person without the permission of the owner accesses or secures access to such computer, downloads any data, introduces any computer contaminant or computer virus into any computer, damages any computer, disrupts any computer network, denies access or causes the denial of access to any person authorised to access any computer, provides any assistance to any person to facilitate access to a computer charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, he shall be liable to pay damages by way of compensation not exceeding 1 crore to the person.

2. Compensation for failure to protect data

- If a body corporate handling any sensitive personal data or information in a computer resource which owns is negligent in implementing and maintaining reasonable security practices such body shall be liable to pay damages to the aggrieved party.

3. Penalty for failure to furnish information return

- If any person who is required under this act should furnish any document , return to the controller or the CA fails to furnish the same , he shall be liable to a penalty not exceeding 150000 for each such failure.

4. Residuary penalty

- Whoever contravenes any rules or regulations made under this act, shall be liable to pay a compensation not exceeding 25000 to the person affected by such contravention.

5. Power to adjudicate

6. Factors to be taken into account by the adjudicating officer

- The amount of gain of unfair advantage, wherever quantifiable made as a result of the default.
- The amount of loss caused to any person as a result of the default.
- The repetitive nature of the default.

The cyber regulations appellate tribunal

- Establishment of cyber appellate tribunal.
- Composition of cyber appellate tribunal.
- Qualification for appointment as presiding officer of cyber appellate tribunal.
- Term of office.
- Salary, allowances, and other terms and conditions of service of presiding officer.
- Filling up of vacancies.
- Resignation and removal.
- Orders constituting appellate tribunal to be final.
- Staff of the cyber appellate tribunal.
- Appeal to cyber appellate tribunal.
- Procedure and powers of the cyber appellate tribunal.

- Right to legal representation.
- Limitation.
- Civil court not to have jurisdiction.
- Appeal to high court.
- Compounding of contraventions.
- Recovery of penalty.

Offences

1. Tampering with computer source documents

- Whoever knowingly or intentionally conceals, destroy or alters or intentionally or knowingly causes another to conceal, destroy any computer source code used for a computer or computer network, shall be punishable with imprisonment up to three years or with a fine up to 2 lakh or with both.

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 up to 5 lakh or both.

3. Punishment for receiving stolen computer resources 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 for a term which may extend up to 3 years or with fine up to 1 lakh or both.

4. Punishment for identity theft

- Whoever fraudulently or dishonestly make use of electronic signature ,password or 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.

5. 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 3 years and shall also be liable to fine which may extend to 1 lakh rupees.

6. Punishment for violation of privacy

- Whoever, intentionally publishes or transmits the image of a private area of any person without his or her consent, shall be punished with imprisonment which may extend to 3 years or fine not exceeding 2 lakh rupees or both.

7. Punishment for cyber terrorism

- Whoever with intent to threaten the unity, integrity, security of sovereignty of India or any section of the people by- denying or cause the denial of access to any person authorized to access computer resource or attempting to penetrate or access a computer resource without authorization or exceeding authorized access.
- Whoever 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.
- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

8. 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, shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to 1 lakh.

9. Punishment for publishing or transmitting of material containing sexually explicit act in electronic form

- Whoever publishes or transmits or causes to be published in the electronic form any material which contains sexually explicit act or conduct shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to 10 lakh rupees.

10. Power of controller to give directions

- The controller may, by order, direct a CA 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 made thereunder.
- 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 3 years or to a fine not exceeding 2 lakh or to both.

11. Government agency power to intercept information

- The act empowers the central/ state government authorised agency to intercept, monitor or decrypt any information generated, transmitted or stored in any computer resource if it is deemed fit in the interest of the sovereignty .
- The agency can also secure all the facilities and technical assistance from the subscriber or computer personnel to decrypt the information.
- The subscriber or any person who fails to assist the agency shall be punishable with an imprisonment for a term to 7 years.

12. Protected system

- The appropriate government may, by notification in the official gazette, declare any computer, computer system or computer network to be a protected system.
- The appropriate government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section 1.
- 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 up to 10 years and shall be liable to fine.

13. Penalty for misrepresentation.

- Whoever makes any misrepresentation to, or suppresses any material fact from, the controller or the CA for obtaining any licence or digital signature certificate, as the case may be, shall be punished up to 2 years or with fine which may extend to 1 lakh or both.

14. Penalty for breach of confidentiality and privacy

- Any person who, in pursuance of any of the powers conferred under this act, rules or regulation made thereunder, has secured access to any electronic record, book, register or other material without the consent of the person concerned, discloses such electronic record or other material to any other person shall be punished up to 2 years of imprisonment or fine with 1 lakh or both.

15. Penalty for publishing digital signature certificate false in certain particulars

- No person shall publish a DSC with the knowledge that the CA listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it.
- Any person who contravenes the provisions of sub section 1 shall be punished up to 2 years imprisonment or fine with 1 lakh or both.

16. Publication for fraudulent purpose

- Whoever knowingly creates, publishes or otherwise makes available a DSC for any fraudulent shall be punished up to 2 years of imprisonment or fine with 1 lakh or both.

17. Act to apply for offence or contravention committed outside India

- Subject to the provisions of subsection 2, the provisions of this act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.
- Subject to the provisions of subsection 2, the provisions of this act shall apply also to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer located in india.

18. Confiscation

- Any computer, computer system, floppies, CD, 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.

19. 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.

20. 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.

Miscellaneous provisions

1.Power of police officer and other officers to enter search

- Notwithstanding anything contained in the code of criminal procedure 1973, a police officer not below the rank of deputy superintendent of police, or any other officer authorised by the central government, 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.

- Where any person is arrested 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.

2. Act to have overriding effect

3. Controller, deputy controller, and assistant controllers to be public servants

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.

5. Protection of action taken in good faith

6. Offences by companies

- 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.

7. Removal of difficulties

- 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 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.
- Every order made under this section shall be laid, as soon as possible after it is made, before each house of parliament.

8. Constitution of advisory committee

- The central government shall, as soon as possible after the commencement of this act, constitute a committee called the cyber regulations advisory committee.
- The cyber regulation 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 govt.

9. Special provisions for evidence relating to electronic record

10. Admissibility of electronic records

11. Presumption as to electronic records and digital signatures

- In any proceeding 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.
- In any proceeding, involving a secure DS, the court shall presume, unless contrary is proved, that the secure DS is affixed by subscriber with the intention of signing or approving the electronic record.

12. Presumption as to digital signature certificates

13. Presumption as to electronic messages

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

THANK YOU