CH.15th : Law relating to Information Technology.

* Objective

1) To provide legal recognition for transactions
2) To provide legal recognition & facilitate filing of documents.
3) To amend the same acts so as to provide / bring electronic documentation within purview of respective enactments.
4) To provide legal recognition to digital signature
5) To provide legal recognition for storing data.
6) To give legal recognition for keeping books of accounts in electronic form.
7) facilitating electronic fund transfer.
8) To stop computer crime & protect privacy of internet users.

* Documents / Transaction to which the act shall not apply :-
1) Negotiable instruments
2) Trust
3) Power - of - attorney
4) Will
5) Contract of & sale of immovable property.

* IMP Definations :-

1) Addressee :- Person who receives electronic record.

2) Asymmetric Crypto System

↓

means system of secure key pair

↓

it is consists of

Private key & Public key

↓ ↓

for creating digital signature — to verify digital signature.

3) Electronic signature : It means authentication of any electronic record by subscriber by means of electronic technique specified in 2nd schedule and includes digital signature.

4) Originator : Person who sends electronic document/ message.

* DIGITAL SIGNATURE & ELECTRONIC SIGNATURE.

i) Any subscriber can authenticate electronic record by affixing his digital signature. Authentication can be done by using "asymmetric cryposystem & hash function."

ii) Verification of electronic record done by use of public key of subscriber

iii] Any change made to the document after it is signed, then signature will be invalid. It helps to protect from forgery & tampering. Hence, digital signature helps to maintain the authenticity & integrity of document.

iv] Digital signature has legal recognition in India. Under Income Tax Act & GST Laws, a person can sign returns & documents electronically by attaching digital signature.

v] Electronic Record can be authenticated by subscriber by such electronic signature which is considered reliable & specified & 2 in 2nd schedule.

vi] Electronic signature considered reliable if -
- Signature is within the context
- at the time of signing signature is under the control of signatory
- Any alteration to electronic signature made after affixing signature is detectable.
- Any alteration to information made after its signature is detectable
- & if it fulfills conditions as may be prescribed.

* ELECTRONIC GOVERNANCE

- Sec 4 : Any information in writing / in typewritten form or in printed form can be made or rendered in electronic form & can be accessable for subsequant reference.

- Section 5 : This section states that instead of physically signing a paper or document, people can use electronic device i.e. it can be signed electronically to confirm or verify the document.

- Sec. 6 : filing of any form, application or other documents, creation, retention or preservation of records, payment to govt. offices or agencies can done through electronically.

- Sec. 7 : Retention of information
  It states that some information, document or record can be retained for specific period. Certain conditions are need to be followed.
  1) Information shall be made available for subsequent reference.
  2) Electronic record shall be retained in format in which it was originally generated, sent or received.
  3) All the required details available in electronic record.

- Sec. 7A : This section states that, if there is a law that allows for audit of documents, records or information, then this rule will also apply to the information that are stored & maintained ~~managed~~ electronically.

* Difference between Electronic Signature & Digital Signature

Points	Electronic Signature	Digital Signature.
i) Meaning	It is a digital form of weblink signature which is legally binding & secure.	It is a secured signature that works with electronic signature & relies on public key.
ii) Purpose	It is used for verf verifying document	It is used for securing document.
iii) Validation	It does not require validation.	It has validation
iv) Security	It is vulnerable for to tampering as there is fewer security features.	It is highly secured & has more security features.
v) Verification	Electronic signature cannot be verified.	Digital Signature can be verified.
vi) Types	Verbal, electronic ticks & scanned signature.	Types of digital Signature includes Adobe & microsoft.
vii) Utility	It is simple to use but it has lesser level of evidential value.	Generally, it is preffered because of more authenticity

- Section 8 : Subordinate legislation can also pub- in the official Gazette or electronic Gazette. The date when it is first published in either of these Gazettes will be considered as official date of publication.

- Section 9 : The provisions mentioned above do not give anyone the power to demand that a government agency accept, issue or carry out any document or ~~fina~~ monetary transaction in electronic form.

- Section 10 : If any contract is expressed in electronic form or by means of electronic record, then it cannot be considered invalid just because it was done electronically

- Section 11 : Attribution & Dispatch of Electronic records
  Electronic record is attributed to originator
  1) If it is send by originator himself, OR
  2) Sent by person authorised to act on behalf of originator OR
  3) If it is sent by information system programmed by originator to operate ~~auto~~ automatically

* Time & Place dispatch Etc

- Time of dispatch
  Time of dispatch should be as per agreement
  If there is no agreement then when e-record enters a computer resource outside the control of originator

- Time of Receipt
When the electronic record enters the computer resource of the addressee.

* SECURE ELECTRONIC RECORDS
Electronic signature will be considered secure if
- at time affixing signature it was under the control of signatory.

- signature creation data was stored & affixed in such manner as prescribed.

- If signature creation data is in control of two or more person then it cannot be deemed to be secure electronic signature.

* CERTIFYING AUTHORITIES
A Certifying Authority is a trusted body whose central responsibility is to issue, revoke, renew & provide directories of Electronic Certificates.

Certifying Authority means a person who has been granted license to issue Electronic Signature Certificates.

* Procedure of obtaining electronic signature certificate

- A person can make application to certifying authority to issue electronic signature certificate with fees

• Then after consideration certifying Authority after making enquiries will grant electronic signature certificate. And if rejected application then will gives reasons for it.

* APPELLATE TRIBUNAL

~~Sec. 57~~

Sec. 57 : Any person aggrieved by order of Controller or Certifying authorities, then can appeal to Appellate tribunal within 45 days.

Any person aggrieved by "any decision or order", may appeal to ~~High~~ High Court within 60 days.

* PENALTY

Section 43: Provides that if any person without permission of owner or any other person who is in charge of computer or computer network

1) Accesses or secures access to computer system

2) downloads, copies or extracts any data, computer data base or information from computer system

3) introduces or causes to be introduced computer virus into computer system.

4) damages or causes to be damaged computer system

5) Disrupts or causes to be disruption of computer

6) Denies or causes the denial of access to any person authorised to access any computer system.

7) Provides any assistance to any person to facilitate access to computer system in contravention of provisions of this act & rules made thereunder

8) Tampers or manipulates computer system

9) Destroys or deletes any information residing in computer system

10) Steal, conceal, destroys or causes to steal, conceal, destroy computer system

* Section 66 : If any person does act referred to Sec. 43, then he shall be punishable with 3 years imprisonment or 5 Lakh Rs fine or both

* Computer related offences
The offences listed in Act, are following -

1) Dishonestly stolen computer resource or device

2) Identity theft

3) Cheating by personation by using computer resource.

4) Violation of privacy.

5) Cyber terrorism

6) Publishing or transmitting of material containing sexually explicit.

7) Publishing or transmitting of material containing depicting children in sexually explicit.

8) Misrepresentation

9) Breach of confidentiality & privacy

10) Disclosure of information in breach of lawful contract.

11) Publishing electronic signature certificate false in certain particulars.

12) Publication for fraudulent purpose.

* Section 69 :- Central govt. or state govt. can direct any agency to intercept, monitor, decrypt any information generated transmitted, received or stored in any computer resource.

* Section 45 :-

a) If someone fails to file any document, report, or return to certifying authority or controller, then liable to penalty of ₹ 1,50,000 lakh for each failure

b) If person fails to file any return or report, book or any information within prescribed time, he shall be liable with penalty of ₹5000 for each day during which such failure continues.

c) If fails to maintain books of accounts or records, he shall be liable to pay penalty of Rs. 10,000/- every day during which failure continues.

* Compensation for failure to protect data.
Sec. 43A :
When a body corporate handling any sensitive personal data in computer resource which it owns, controls is negligent in implem maintaining resonable security practices & thereby causes wrongful loss to any person, then such Body corporate is liable to pay damages by way of compensation to the person.

* Section 46 : Whoever contravenes any rules & or regulation made under this act & where no penalty is separately provided, then he shall be liable to pay penalty of ₹ 25,000/-.

* Section 65 : Whoever knowingly or intentionally conceals, destroys or alters any computer source, then shall be punishable with imprisonment of 3 years or Rs. 2 lakh fine or both.

* Exemption from liability of intermidiary in certain cases

- Intermediary shall not be liable for any third party information, data or communication link made available or hosted by him.
- If function of intermediary is limited to providing access to communication system
- Intermediarty observes due deligence while discharging their duties

* INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES & PROCEDURES & SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011

- In KS Puttaswamy V. Union of India it was held by Supreme Court that the Right to Privacy is also fundamental Right
- following are considered as sensitive personal information - 1) Password
  2) Bank Account Details
  3) Credit card / Debit card details
  4) Past & Present health records
  5) Sexual orientation
  6) Biometric Data
- A person has certain rights over the sensitive

personal information, this information cannot be collected without provider's consent

- Privacy policy
- Consent
- Collection limitation
- Notice
- Retention limitation
- Purpose limitation
- Right to access & correct
- Right to withdraw consent 'opt out'
- Grievance officer
- Disclosure with consent, Prohibition on publishing & further disclosure
- Requirements for transfer of Sensitive personal Data.
- Security of information.