Page No.:
Date:

Chapter : 19

Law relating to Information Technology

Information Technology is used for any computer, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange of all form of electronic media.
It's a boon for world which provides easy access / transfer of information with other benefits, it also has some negative consequence with the intention to reduce the negative impact of IT, The Information Technology Act was enacted. It also applies to any offences committed outside India by any person.

Objective -

1. To provide legal recognition to transaction carried out by electronic data interchange or as electronic commerces.
2. To facilitate electronic filing of documents with government.
3. To amend the IPC, Evidence Act, RBI Act and various other laws.
4. Provide recognition to digital signature
5. Storing data in electronic format.
6. Facilitating electronic fund transfer
7. To stop computer crime and protect privacy of internet user including data theft.

Page No.:
Date:

Documents / Transactions to which the Act shall not apply :-

1. A negotiable instrument (except a cheque) as defined under Negotiable Instrument Act 1881
2. A power of attorney
3. A trust defined under The Indian Trust Act
4. A will defined in Indian succession Act.
5. Any contract of sale of immovable property or any interest in such property.

Asymmetric crypto system :-

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

Electronic signature :-

means authentication of electronic records by subscriber by means of electronic technique specified in schedule II and includes digital signature.

Digital signature :-

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

Digital Signature & Electronic Signature :-

Any subscriber can authenticate the electronic

record by affixing his digital signature, it is effected by the use of "asymmetric crypto system and hash function."

> verification of documents is done by the use of key pairs.

> Any changes made to the document after it is signed invalidates the signature. This helps to protect information and document from forgery and tampering.

Any electronic signature or electronic authentication technique shall be considered reliable if -

① the signature creating data or authentication data are within the context in which they are used.

② the data were at the time of signing, under the control of the signatory.

③ any alteration to electronic signature made after affixing such signature is detectable.

④ any alteration to information made after authentication is detectable.

⑤ fulfill other condition as may prescribe.

Electronic Governance -

The Act grants legal recognition to electronic records by laying down that such information or any other matter is to be in -

→ writing or
→ typewritten form or
→ printed

Page No.:
Date:
YOUVA

Legal Recognition of Digital Signature :-

where the law provides that information shall be authenticated by affixing the signature, then such requirement shall be deemed to have been satisfied if such information is authenticated by means of electronic signature

Use of Electronic Records -

Filing of any form, application or other document, creation, retention or preservation of records, grant of any license or receipt or payment in any gov. offices may be done through the means of electronic form.

According to section- 6A
Appropriate gov. has authority to authorise service provider to establish, maintain and upgrade computerised facilities for delivering services to the public through electronic means

Retention of Information :-

The Act also seek to permit the retention of information in electronic form, where law provides that certain document retained for any specific period. The conditions are-

> The information contained therein remains reasonable accessible for subsequent reference

> Record is retained in the original format as it was generated, sent or received
> The details of such electronic record are available in electronic record.

Audit of document maintained in Electronic form:-

If there is a provision for audit of document records or information, that provision shall also be applicable for audit of document or information processed and maintained in electronic form

Subordinate legislature:-

The Act to be published in the official Gazette or in electronic Gazette and the date of its first publication in either of the two document shall be deemed to be the date of publication.

Validity of document formed through Electronic means:-

When the contract is formed by means of electronic form, the communication, acceptance, revocation of proposal are expressed by means of an electronic record. Such contract are enforceable in law.

Page No.:
Date:

Attribution and Dispatch of Electronic Record- (Section- 11)

An electronic record is attributed to the originator -

→ if it was sent by originator himself
→ if it was sent by a person authorised to act on his behalf.
→ if it was sent by an information system program.

> Acknowledgement can be made through any communication or conduct from addressee
> If originature requires acknowledgement and it is not received record is deemed unsend.
> If acknowledgement isn't received within a reasonable time originator can notify addresse and if still not received originator may treat the record unsend.

Time and Place of dispatch etc-

The time of dispatch should be :-
As per the agreement between the originator and addressee.
If there is no agreement then dispatch of electronic record deem to occur when e-record enters a computer resource outside the control of originator.

The time of receipt of electronic record occur when record enters the computer resource of the addressee.

> If addressee has designated specific computer resource, receipt occurs when e-record enters that resource.
> If there is no such specific resource receipt is deemed to occur when e-record enters any computer resource.

Secure electronic Records -

An electronic signature shall be deemed to be a secure electronic signature if -
> the signature data, at the time of affixing signature was under the exclusive control of signatory and no other.
> Signature data was stored & affixed in such manner as prescribed.

Certifying authorities -
It's a trusted body whose central responsibility is to issue, revoke, renew and provide directories of electronic certificates.
→ To regulate Certifying authorities controller is appointed by government to promote and for growth of
- E-commerce
- E-governence
- and control of all certifying authorities

Procedure for obtaining electronic signature Certificate -

Any person may make an application in

prescribed form to certifying authority with prescribed fees.
- Every such application shall contain certification practice statement and if no such statement then particulars as may be specified by regulation.
- On receipt of application certifying authority may grant electronic signature certificate or for reasons to be recorded in writing reject the application.
- It may be noted that no application shall be rejected unless applicant has been given opportunity of showing cause against such proposed cause.

Extraterritorial operation

The provisions of this Act shall apply on any offence or contravention committed outside India by any person, if the act or conduct in question involves a computer or computer network located in India.

Suspension of Digital Signature certificate -

→ On receipt of application by subscriber or authorised person.
→ Certifying authority is in opinion to suspend DSC in public interest.
→ Should not be suspended for more than 15 days unless subscriber has given OOBH.
→ On suspension certifying authority shall communicate to the subscriber.

Page No.:
Date:

Revocation of digital Signature certificate

→ Upon death of subscriber
→ Dissolution of firm or winding up.
→ On request of subscriber

Certifying authority may revoke DSC at any time if it is opinion that-

- Material fact is false or has been concealed.
- Requirement are not satisfied
- Subscriber becomes insolvent

Before revocation shall give OOBH.

Adjudicating officer-

Adjudicating officer is appointed by central Government for adjudication.
He may impose penalty or award compensation
He shall check-

> Amount of unfair gain / advantage
> Amount of loss caused to a person
> Repetative nature of default.
> Matter shall not exceed ₹ 5cr.

Following data shall not be disclosed-

> Password
> Bank a/c details
> Credit / Debit card details
> Present and past health records
> Sexual orientation
> Biometric data.