

Chap 10 - INFORMATION TECHNOLOGY (AMENDED) ACT, 2008

- Brief History
- The IT Act 2000 And It's Objectives
- Preliminary [Chapter I]
- Digital Signature And Electronic Signature (Amended Vide ITAA 2008) [Chapter-II]
- Electronic Governance [Chapter III]
- Attribution, Acknowledgment And Dispatch Of E-record s [Chapter IV]
- Secure E-record s And Secure Electronic Signatures [Chapter V]
- Regulation Of CA [Chapter VI]
- ESCs [Chapter VII]
- Duties Of Subscribers [Chapter VIII]
- Penalties And Adjudication [Chapter IX]
- The Cyber Appellate Tribunal (Amended Vide ITA-2008) [Chapter X]
- Offences [Chapter XI]
- Intermediaries Not To Be Liable In Certain Cases (Substituted Vide ITA-2006) [Chapter XII]
- Miscellaneous [Chapter XIII]

- ❖ **WHERE-** Where any law provides that _
- ❖ **THEN-** Then such requirement shall be deemed to be satisfied if

IT (Amendment) Bill 2006 was amended by IT Act Amendment Bill 2008 and in the process, the underlying Act was renamed as IT (Amendment) Act 2008 herein after referred to as ITAA 2008.

Reasons for Amending IT Act

1. To include new types of Cyber crimes
2. To increase protection of personal data & info. for national security, economy, public health & safety
3. To provide for alternate technology for e-Signatures as per Model Law UNCITRAL
4. To authorize Service Providers providing services to SG/CG

OBJECTIVES

- ❖ State the objectives and scope of IT Act, 2000. (May-05, Nov-07, RTP)
1. Legal recognition for *transactions* carried out by means of **E-data interchange** (EDI), **E-Commerce**
 2. Facilitate and legalize **E-fund transfers** (EFT)
 3. Facilitate **E-storage** of data
 4. Facilitate **E-filing** of documents with Govt departments
 5. Legal recognition for keeping of **books of accounts** by bankers in **E-form**
 6. Legal recognition to **Digital signatures** for authentication of information
 7. Amend RBI Act, Banker's Book Evidence Act, Indian Evidence Act, Indian Penal Code

DEFINITIONS

- ❖ What is a Digital Signature? (Nov-02) [Hint: Refer Annexure]
- ❖ Short notes: Digital Signature Certificate (Nov-03)
- ❖ Define: Affixing digital signature; Asymmetric crypto system; Computer network; Private & Public keys; Secure system (Nov-04)
- ❖ Define following terms: Information; Electronic form; Data; Key pair; Adjudicating officer (RTP)

- a) **Access** means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network
- b) **Addressee** means a person who is intended by the originator to receive the E-record. Excludes intermediary
- c) **Adjudicating officer** (AO) means an adjudicating officer appointed under the Act
- d) *** Affixing Electronic signature** means adoption of any methodology or procedure by a person for authenticating an E-record via electronic signature
- e) *** Asymmetric crypto system** means a system of a secure key pair consisting of a private key for creating a *digital* signature and a public key to verify the *digital* signature
- f) *** Certifying Authority (CA)** means a person who has been granted a licence to issue an ESC under the Act
- g) **Certification practice statement** is issued by a CA to specify the practices that it employs in issuing ESCs
- h) **Communication Device means** Cell Phones, Personal Digital Assistance (PDAs), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image
- i) **Computer** (C) 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 IPO, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network
- j) **Computer network** (CN) means the interconnection of one or more computers through-
 - o the use of satellite, microwave, terrestrial line or other communication media
 - o terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained
- k) **Computer resource** (CR) means computer, computer system, computer network, data, computer data base or software
- l) **Computer system** (CS) means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions
- m) **Controller** means the Controller of CA appointed under the Act

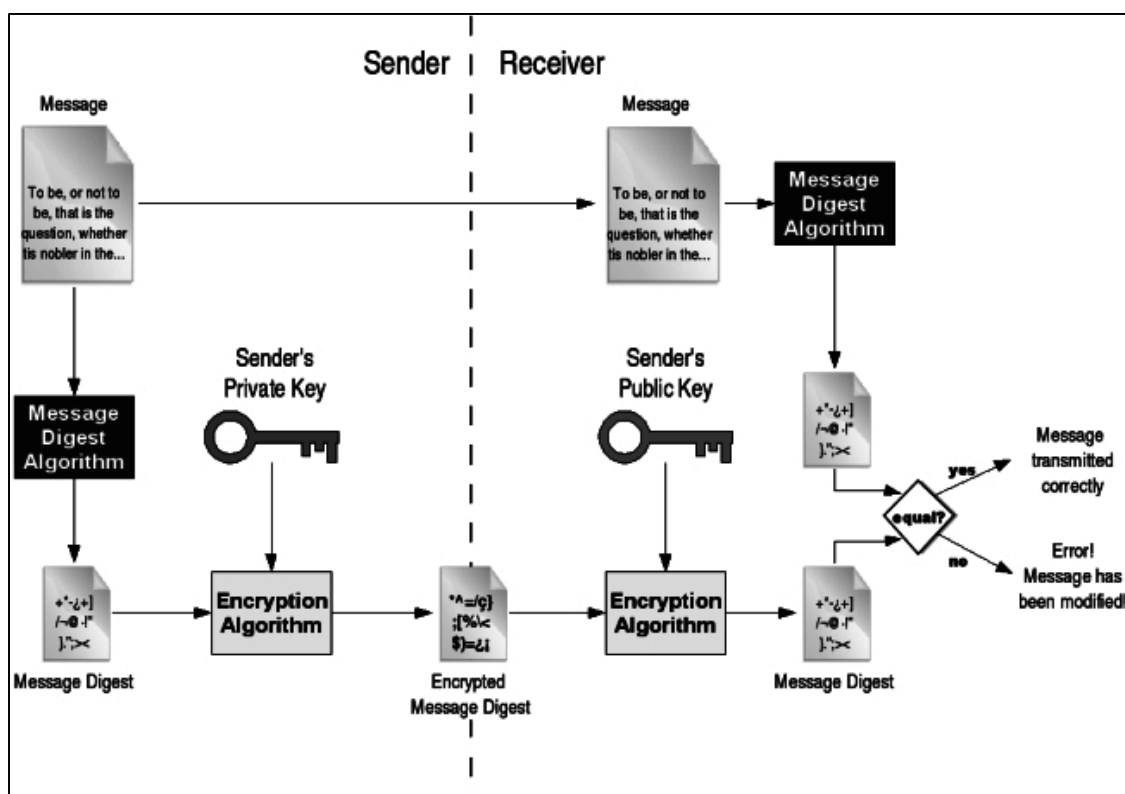
- n) **Cyber Appellate Tribunal** (CAT) means the Cyber Appellate Tribunal established under the Act. (X “Regulation” or CRAT)
- o) **Cyber Café** means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public
- p) **Cyber Security** means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction
- q) **Data** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in 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
- r) *** Digital signature** means authentication of any E-record by a subscriber by means of an electronic method or procedure in accordance with the Act
- s) *** Digital Signature Certificate** means a Digital Signature Certificate issued under the Act
- t) **Electronic form** with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device
- u) **Electronic Gazette** means the Official Gazette published in the electronic form
- v) *** E-record** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche
- w) *** Electronic signature** means authentication of any e-record by a subscriber by means of the e-technique specified in the 2nd schedule and includes digital signature
- x) *** Electronic signature certificate** means an ESC issued under Sec 35 and includes Digital Signature Certificate
- y) **Function** in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer
- z) **Indian Computer Emergency Response Team** means an agency established the Act
- aa) **Information** includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche
- bb) *** Intermediary** with respect to any particular e-record s, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.
- cc) *** Key pair** in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key

- dd) **Licence** means a licence granted to a CA under the Act
- ee) * **Originator** means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person. Excludes intermediary
- ff) **Prescribed** means prescribed by rules made under the Act
- gg) * **Private key** means the key of a key pair used to create a digital signature
- hh) * **Public key** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate
- ii) * **Secure system** means computer hardware, software, and procedure that-
- o are reasonably secure from unauthorised access and misuse
 - o provide a reasonable level of reliability and correct operation
 - o are reasonably suited to performing the intended functions
 - o adhere to generally accepted security procedures
- jj) **Security procedure** means the security procedure prescribed under the Act by the Central Govt
- kk) * **Subscriber** means a person in whose name the ESC is issued
- ll) * **Verify** in relation to a digital signature, e-record or public key means to determine whether-
- o the initial E-record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber
 - o the initial E-record is retained intact or has been altered since such E-record was so affixed with the digital signature

DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (AMENDED - ITAA 2008)

This chapter (contains Sec 3) gives legal recognition to E-records and digital signatures. The Sec provides the conditions subject to which an E-record may be authenticated by means of affixing digital signature.

❖ How is it (Digital Signature) used? (Nov-02)



The digital signature is created in two distinct steps.

- 1) First, the E-record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the E-record thus ensuring the integrity of the content of the E-record.
 - a) Any tampering with the E-record will invalidate the digital signature
- 2) Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key.
 - o It helps to verify whether the E-record is retained intact or has been tampered with
 - o It helps the person with the public key to identify the originator of the message

Sec-3: Authentication of E-records

1. Any subscriber may authenticate an e-record by affixing his Digital Signature.
2. The authentication of the e-record shall be effected by the use of asymmetric crypto system and hash function* which envelop and transform the initial e-record into another e-record
3. Any person by the use of a public key of the subscriber can verify the e-record
4. The private key and the public key are unique to the subscriber and constitute a functioning key pair

* "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 E-record yields the same hash result every time the algorithm is executed with the same E-record as its input, making it computationally infeasible-

- o to derive or reconstruct the original E-record from the hash result produced by the algorithm
- o that two E-records can produce the same hash result using the algorithm

(-Hash function vs. Hash result-)

Sec-3A: Electronic Signature

A subscriber may authenticate any e-record by such e-signature or e-authentication technique which:

- (a) is considered reliable** and
- (b) may be specified in the 2nd Schedule

** If-

- (a) the signature creation data or the authentication data are **linked** to the signatory or the authenticator and of no other person
- (b) the signature creation data or the authentication data were, at the time of signing, under the **control** of the signatory or the authenticator and of no other person;
- (c) any alteration to the e-signature made after affixing such signature is detectable
- (d) any alteration to the information made after its authentication by e-signature is detectable
- (e) it fulfills such other conditions which may be prescribed

The Central Government may prescribe change to any technique/procedures via official Gazette

Electronic Governance

- ❖ Discuss the main provisions provided in IT Act, 2000 to facilitate E-Governance (Nov-08)
- ❖ Explain Electronic Governance (RTP-Final New)

This chapter specifies the procedures to be followed for 1) sending and receiving of E-records and 2) time and the place of the dispatch and receipt. It provides for the following:

Sec-4: Legal recognition of E-records

WHERE- information or any other matter shall be in *writing* or in the *typewritten* or *printed* form

THEN- if it is-

- rendered or made available in an e-form; and
- accessible so as to be usable for a subsequent reference

Sec-5: Legal recognition of Digital Signatures

WHERE- any information or matter should be authenticated by affixing the signature or any document should be signed or bear the signature of any person,

THEN- if it is authenticated by means of Digital Signatures affixed in the prescribed manner

“Signed” with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression “signature” shall be construed accordingly.

Sec-6: Use of E-Records and E-Signature in Govt. & its agencies

WHERE-

- (a) the filing of any form, application or any other document with any office owned or controlled by the appropriate Government
- (b) the issue or grant of any license, permit, sanction or approval etc.
- (c) the receipt or payment of money

THEN- if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such e-form as may be prescribed by the appropriate Government.

The appropriate Government may prescribe 1) manner and format in which such e-records shall be filed, created or issued; 2) manner or method of payment of any fee or charges

Delivery of Services by Service Provider

The appropriate Government (for efficient delivery of services to the public through e-means) may **Authorize any service provider-**

- To set up, maintain and upgrade the computerized facilities etc.
- To collect, retain and appropriate service charges for services from persons availing such service

And also specify via-Official Gazette charges which may be charged and collected

Sec-7: Retention of E-record s

WHERE- Documents, records or information shall be retained for any specific period

THEN- if such documents, records or information

- are retained in the e-form
- are retained in the original format
- are retained with details (origin, destination, date and time of dispatch or receipt of such e-record)
- accessible so as to be usable for a subsequent reference

Audit of Documents in E-form :

WHERE- provision of audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in E-form.

Sec-8: Publication of rules, regulation, etc, in Electronic Gazette

WHERE- any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette

THEN- if such _ is published in the Official Gazette or E-Gazette:

(Date of Publish - whichever published first in any form)

Sec-9: Sec 6-8 Not to Confer Right to insist document should be accepted in E-form (by Govt. Authorities)

No person can insist _

Sec-10: Power to make rules by Central Government in respect of E-Signature

Prescribe-

- a) *Type of E- Signature*
- b) *Manner and format* in which E-Signature shall be *affixed*
- c) *Manner or procedure which facilitates identification of the person affixing the E-Signature*
- d) Control processes and procedures to ensure adequate CIS of E-records or payments
- e) Other matter needed to give legal effect to E-Signature.

Validity of contracts formed through electronic means

Where in a contract formation, the communication/acceptance/revocation of proposals are expressed in e-form/e-record, such contract shall not be deemed to be unenforceable solely on the ground that such e-form or means was used for that purpose (-it is valid-)

ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF E-RECORDS

'Attribution' means 'to consider it to be written or made by someone'. Hence, this Sec lays down how an e-record is to be attributed to the person who originated it.

Attribution of E-record s

An e-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 e-record; or
3. by an *information system programmed* by or on behalf of the originator to operate automatically.

Acknowledgement of Receipt

- 1) Where the originator **has not** mentioned any form or method of acknowledgment of receipt of e-record, then an acknowledgment may be given by -
 - a) any *communication* by the addressee
 - b) any *conduct* of the addressee indicating that the e-record has been received
- 2) Where the originator **has** _ , then unless acknowledgment has been so received, the e-record shall be deemed to have been never sent by the originator
- 3) Where **time limit** for acknowledgment not mentioned, the originator may give notice mentioning a reasonable time for it

Time and place of despatch and receipt of e-record

--- If not otherwise agreed between the originator and the addressee ---

- **Time of receipt** of an e-record when the e-record =
 - Enters the designated computer resource (designated a computer resource)
 - Is retrieved by the addressee (X designated computer resource)
 - Enters the computer resource of the addressee (XXX designated a computer resource)
- **Dispatch** of an e- record occurs **when** it enters a computer resource outside the control of the originator. An e-record is deemed to be dispatched/received at the **place** where-
 - Originator has his principal place of business (Or usual place of residence/regn.)
 - Addressee has his principal place of business (Or usual place of residence/regn.)

SECURE E-RECORDS AND SECURE E-SIGNATURES [CHAPTER V]

Chapter V - Conditions that would apply to qualify e-records & digital signatures as being secure

Sec 14: Secure E-Record

Where any security procedure has been applied to an e-record at a specific point of time, then such record shall be deemed to be a secure e-record (from such point of time to the *time of verification*)

Sec 15- Secure E-signature

An e-signature shall be deemed to be a secure e-signature if signature creation data was-

1. under the exclusive control of the signatory and no other person
2. stored and affixed in a manner that has been prescribed

("signature creation data" means the private key of the subscriber)

Sec 16 - Security procedure and practices

CG may prescribe the security procedures and practices taking due regard to the commercial circumstances, nature of transactions related factors

REGULATION OF CA [CHAPTER VI]

Chapter VI - provisions relating to the appointment and powers of the Controller and CA

Sec 17: Appointment of Controller and other officers (Amended Vide ITAA 2008):

- CG may appoint a Controller, Deputy and Assistant Controllers, officers etc.
- Deputy and Assistant Controllers, officers etc. < Controller < CG
- Qualifications, experience and T&C of service
- Seal of the Office of Controller

Sec 18: Controller may perform all or any of the following functions (Functions of controller)

With respect to E-Certificates-

- 1) Specifying the form and content of a ESC and the key
- 2) Specifying the content of Advt. for ESC and the Public Key

With respect to CA-

- 1) Exercising supervision over their activities
- 2) Specifying the conditions for conducting their business
- 3) Specifying the qualifications and experience of their employees
- 4) Laying down their duties and the standards to be maintained by them
- 5) Specifying how Accounts will be maintained
- 6) Specifying the T&C for appointing/remunerating auditors
- 7) Certifying their public keys
- 8) Facilitating the establishment of their electronic system
- 9) Maintaining a data-base containing their disclosure record
- 10) Manner in which they shall conduct their dealings with the subscribers
- 11) Resolving any conflict of interests between them and the subscribers

Sec 19: Recognition of foreign CA

- The Controller may recognize (via- CG + Gazette) any foreign CA & ESC issued by them will be valid
- The Controller may revoke such recognition

Sec 21: License to issue ESCs (ESC)

- Any person may make an application to the Controller for a licence to issue ESC
- Applicant MUST fulfill requirements- qualification, expertise, manpower, financial resources and other infrastructure facilities etc.
- Licence granted will 1) valid for a specified period 2) not be transferable or heritable 3) subject to T&C

Sec 22: Application for license

Every application shall be made in a CG prescribed form with necessary documents (A certification practice statement etc.) & fees

Sec 23: Renewal of license

Every application shall be made in a CG prescribed form at least forty-five days before the date of expiry and with fees

Sec 24: Procedure for grant or rejection of license

The Controller may as he deems fit grant the licence or reject the application with reasonable opportunity of presenting his case. Appropriate notices, show cause

Sec 25: Suspension of License

The Controller may suspend a licence, after giving opportunity of showing cause if the CA has:

- Made a statement which is incorrect or false
- Failed to comply with the T&C or standards
- Contravened any provisions

Sec 26: Notice of suspension or revocation of license

The Controller shall publish notice in the maintained data-base / repositories when the licence is suspended or revoked

Sec 27 - Power to delegate

The Controller may authorise the Deputy or Assistant Controller or any officer to exercise any of his powers

Sec 28 - Power to investigate contraventions

The Controller or any authorized officer shall have powers which are conferred on income-tax authorities

Sec 29 - Access to computer and data

The Controller or any authorised person shall have access to any system and able to direct any person in charge of the system for investigation/information search

Sec 30 - Duties of CA

Every CA shall follow certain procedures in respect of Digital Signatures.

- Make use of hardware, software, and procedures that are *secure from intrusion and misuse*
- Adhere to security procedures to assure that the *secrecy and privacy* of the E-Signature
- Provide a reasonable level of *reliability* in its services
- Be the repository of all ESC issued under this Act
- Publish information regarding its practices, ESC and current status of such certificates;
- Observe such other standards as may be specified by regulations.

Sec 31 - CA to ensure compliance of the Act

CA shall ensure that their employees comply with the regulations and orders

Sec 32 - Display of licence

CA shall display its licence at a conspicuous (-noticeable/obvious-) place of business

Sec 33 - Surrender of Licence

CA whose license is suspended or revoked shall immediately surrender the licence. Otherwise- 6m/10k

Sec 34 - Disclosures by CA

- CA shall disclose to subscribers its ESC, certification of practice statement, notice of revocation or suspension and any fact that adversely affects the reliability of its services / issued ESC
- Where any event occurs that _ , then also notify.

ELECTRONIC SIGNATURE CERTIFICATES [CHAPTER VII]

Sec 35 - CA to issue ESC

- Any person may apply to CA for the issue of a ESC with fees which may vary for different services
- CA may grant the Certificate or reject the application after opportunity of showing cause
- Applicant will be given the private key corresponding to the listed public key

No DSC shall be granted unless CA satisfied that-

1. Applicant holds the private key corresponding to the public key to be listed in the DSC
2. Applicant holds a private key, which is capable of creating a digital signature ^ ^
3. Public key to be listed can be used to verify a digital signature affixed by the applicant's private key
^ ^

Sec 36 - Representations upon issuance of DSC

A CA while issuing a DSC shall certify that-

1. It has complied with the Act
2. It has issued the DSC and the subscriber has accepted it
3. Subscriber holds the private key corresponding to the public key listed in the Certificate (^ ^)
4. Subscriber's public key and private key constitute a functioning key pair
5. Information inside DSC is accurate
6. X adversely affect the reliability of the representations

Sec 37 - Suspension of electronic certificates

CA may suspend e-Certificate issued by it after opportunity of being heard-

- Upon request from the subscriber or person authorised by subscriber
- In the public interest

Sec 38 - Revocation of ESC

A CA may revoke an ESC issued by it after opportunity of being heard-

1. Upon request from the subscriber or person authorised by subscriber
2. Upon death of the subscriber
3. Upon the dissolution/winding-up/insolvency of the subscribing firm
4. Fact represented in the ESC is false or has been concealed
5. Requirement for issuance of the ESC was not satisfied
6. Private key or security system was compromised

Sec 39 - Notice of suspension or revocation

The CA shall publish a notice of suspension or revocation of ESC & communicate to subscriber

DUTIES OF SUBSCRIBERS [CHAPTER VIII]

Sec 40 - Generating key pair

On acceptance of ESC the subscriber shall generate the key pair

Sec 40A - Duties of subscriber of ESC

In respect of ESC the subscriber shall perform prescribed duties

Sec 41 - Acceptance of DSC

Subscriber *deemed to have accepted DSC* if he publishes or authorizes to publish the ESC-

- To one or more persons
 - In a repository
- Or otherwise demonstrate approval of DSC

By accepting, Subscriber certifies-

1. Information provided to CA and that which is contained in the ESC to be TRUE
2. Certifies that he holds the private key corresponding to the public key listed in the Certificate & is entitled to do so

Sec 42 - Control of private key

Every subscriber shall exercise-

1. reasonable care to retain control of the private key
2. take all steps to prevent its disclosure

If the private key has been compromised the subscriber will be liable till he has informed the CA

PENALTIES AND ADJUDICATION [CHAPTER IX]

Sec 43 - Penalty and compensation for damage to computer, computer system or network

If any person *without permission* of the owner or any other person who is in-charge of a C-CS-CN -

1. Accesses or secures access to such _____
2. Denies access to authorized person to such _____
3. Downloads, copies or extracts any data, database or information from such _____, storage medium
4. Introduces any computer contaminant or computer virus into such _____
5. Damages / Disrupts such _____
6. Destroys, deletes or alters any information residing in a computer resource or diminishes its utility
7. Charges the services availed of by a person to the account of another person by tampering/manipulating such _____
8. Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage
9. Assists any person to facilitate access against the Act

... He shall be liable to pay compensation to person affected

- **Computer Contaminant**- any set of computer instructions that are designed to 1) modify, destroy, record, transmit data or programme residing within ____ 2) usurp the normal operation of ____
- **Computer Database**- representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are prepared by a ____ for use in ____
- **Computer Virus** means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer

resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource

- **Damage** means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means
- **Computer Source code** means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form

Sec 43A - Compensation for failure to protect data

A body corporate handling any sensitive personal data is in a ___ which it owns/controls/operates-

- Negligent in maintaining reasonable security practices > thereby causes loss or gain to any person > liable to pay damages to the person so affected

Reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment (agreement/law/CG)

Sec 44 - Penalty for failure to furnish information, return

Required but-

- Fails to furnish any document, return or report to Controller or CA (1.5L)
- Fails to file any return or furnish any information within the time specified (5k/day)
- Fails to maintain books of account or records (10k/day)

Sec 45 - Residuary Penalty

Penalty for contravening any rule for which no penalty given (25k)

Sec 46 - Power to Adjudicate, Appointment and powers of AO

- CG shall appoint AO for holding an inquiry
- AO to have experience in the field of IT/Legal/Judicial
- Every adjudicating officer shall have the powers of a civil court
- AO shall exercise jurisdiction for claims/damages upto Rs. 5C
- AO may impose such penalty as he thinks fit

Sec 47 - Factors to be taken into account by the AO (in adjudging the quantum of compensation)

- Amount of gain of unfair advantage made as a result of the default
- Amount of loss caused to any person as a result of the default
- Repetitive nature of the default

THE CYBER APPELLATE TRIBUNAL [Chapter X]

Sec 48 - Establishment of Cyber Appellate Tribunal (CAT)

CG shall establish one or more Cyber Appellate Tribunals and specify the matters & places for exercising jurisdiction

Sec 49 - Composition of CAT

CAT = a chairperson, members as selected by CG + Chief Justice

Sec 50 - Qualifications for appointment as chairpersons and members

Chairperson must be qualified to be a HC judge. For details refer Book

Sec 51 - Term of Office of presiding officer

- The chairperson or member shall hold office for a term of 5y or to the age of 65
- Should have no financial or other interest that could be prejudicial
- CG/SG officer must leave service first to be chairperson/member

Sec 52 - Salary and allowances and other terms and conditions

As prescribed

Sec 52A - Powers of superintendence, direction

Chairperson shall have powers of general superintendence & directions. Will preside over Tribunal meetings .

Sec 52B - Distribution of business among benches

Chairperson may order distribution of business among benches

Sec 52C - Powers of the Chairperson to transfer cases

Chairperson may transfer any case pending before one bench, for disposal to any other (Appln/Hearing/Suo moto)

Sec 52D - Decision by majority

In case of divided opinion, decisions made by majority of the all the members who have heard the case

Sec 53 - Filling up of vacancies

CG

Sec 54 - Resignation and removal

Chairperson or member can resign his office with 3m notice or appointment of his successor, whichever is earlier and can be removed by the CG after inquiry (misbehaviour/incapacity) made by a SC Judge

Sec 55 - Orders of tribunal to be final and not to invalidate its proceedings

Appointment of chairperson cannot be questioned because of any defect in the constitution of a the tribunal.

Sec 56 - Staff of the CAT

- CG shall provide officers and employees and decide salaries and terms as it may think fit
- Officers and employees of CAT < Chairperson

Sec 57 - Appeal to CAT

- Any person aggrieved by an order made by a Controller or an AO can file appeal
- Appeal shall be filed within 45d from date of the order otherwise show sufficient cause
- CAT may pass orders thereon as it thinks fit within 6m of appeal
- Forms & fees

Sec 58 - Procedures & Powers of CAT

- Power to regulate its own procedures (e.g. place of sittings) > Code of Civil Procedure
- Same powers as are vested in a civil court
 - o *Summoning* and enforcing the attendance of any person and examining him on *oath*
 - o Requiring the discovery and production of documents or other *e-records*
 - o Receiving evidence on affidavits
 - o Issuing commissions for the examination of *witnesses* or documents
 - o Reviewing its *decisions*
 - o Dismissing an application for default or deciding it ex-parte
 - o Any other prescribed matter
- Every proceeding deemed to be a judicial proceeding

Sec 59 - Right to legal representation

The appellant may either appear in person or authorise one or more legal practitioners

Sec 60 - Limitation

Provisions of the Limitation Act, 1963 shall apply to an appeal made to CAT

Sec 61 - Civil court not to have jurisdiction

No civil court shall have jurisdiction in matters concerning an AO or CAT. Exception- if damages exceeds ITAA's penalty

Sec 62 - Appeal to HC

Any person aggrieved by order of CAT may file an appeal to the HC within 60 days otherwise show sufficient cause (60d+60d)

Sec 63 - Compounding of contravention

- Any contravention under the Act (X Chapter) can be compounded by the Controller or AO provided that such sum shall not exceed the maximum amount of the penalty
- NA- person who commits the same or similar contravention within a period of 3y from the date on which the first contravention, committed by him, was compounded

Sec 64 - Recovery of penalty

A penalty can be recovered as arrear of land revenue and the licences shall be suspended till penalty paid

OFFENCES [CHAPTER XI] (fine or imprisonment or BOTH)

Sec 65 - Tampering with computer source documents

- Destroy, alter, conceal OR causes another to ____ any computer source code, program, network etc.
- *Hacking*- Act of destroying or deleting or altering any info residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the public or that person

Sec 66 - Computer Related Offences

For dishonest or fraudulent action laid out in Sec 43 (Damages to C-CS-CN)

Sec 66A - Punishment for sending offensive messages through communication service

Any person who sends by means of computer resource or comm. device-

- Any information that is grossly offensive or has menacing character
- Any false information for causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will
- Any e-message to deceive or to mislead the recipient about the origin of such messages

E-mail: message or information including attachments in text, image, audio, video and any other e-record

Sec 66B - Punishment for dishonestly receiving stolen computer resource or communication device

Dishonestly receiving or retaining any stolen computer resource or communication device knowing or having reason to believe it is stolen

Sec 66C - Punishment for identity theft

Fraudulently or dishonestly make use of the e-signature, password or any other unique identification feature of any other person

Sec 66D - Punishment for cheating by personating by using computer resource

Cheating by personating (-pretending to be someone-) by means of any communication device or computer resource

Sec 66E - Punishment for violation of privacy (-MMS-)

Intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, violating the privacy of that person

- *Captures*- means to videotape, photograph, film or record by any means
- *Publishes*- reproduction in the printed or e-form and making it available for public
- *Transmits*- electronically send a visual image with the intent that it be viewed by a person or persons
- *Pvt. Area*- naked or undergarment clad genitals, pubic area, buttocks etc.

Sec 66F - Punishment for cyber terrorism *** (-upto Life imprisonment-)

Intent to threaten the unity, integrity, security or sovereignty of India or to strike terror amongst the people by

- Denying or causing denial of access computer resource to persons authorized
- Introducing contaminant & by such conduct-
 - o Causes or is likely to cause death or injuries to persons
 - o Damage or destruction of property
 - o Disrupts essential service or supplies
 - o Adversely affects critical info infrastructure
- Attempting to access computer resource without proper authorization
- Knowingly accesses a computer resource without proper authorization, and thus accesses restricted information for causing 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

Sec 67 - Punishment for publishing or transmitting obscene material in e-form

- Publish or transmit or causes to be published in the e-form, any material which is lascivious or prurient or if its effect is such as to tend to deprave and corrupt persons to read or view

Sec 67A - Punishment for publishing or transmitting material containing sexually explicit act

- Publish or transmit or causes to be published in the electronic form, any material which is sexually explicit act/conduct
- NA- 1) Publication (book, pamphlet, paper, writing, drawing, painting etc) is for public good or in the interest of science, literature, art, or learning etc. 2) kept or used bona fide for religious purposes

Sec 67B - Punishment for publishing/transmitting material depicting children in sexually explicit act

- Publish or transmit or causes to be published in the electronic form, any material which depicts children engaged in explicit act/conduct
- Text/Digital images - Creates, Collects, Seeks, Browse, Downloads, Advertises, Exchanges, Distributes material ____
- Cultivates, Entices or Induces children to online relationship for and on sexually explicit act or other offensive act
- Facilitates abusing children online
- Records in an e-form

NA- 1) Publication (book, pamphlet, paper, writing, drawing, painting etc) is for public good or in the interest of science, literature, art, or learning etc. 2) kept or used bona fide for religious purposes

Sec 67C - Preservation and retention of information by intermediaries

- Intermediary shall retain information for duration and in the manner prescribed by the government
- Intermediary liable if intentionally or knowingly contravenes

Sec 68 - Power of Controller to give directions_

- Controller may direct a CA or its employees to comply with this Act
- Any person who intentionally or knowingly fails to comply with any order would be liable

Sec 69 - Powers to issue directions for interception or monitoring or decryption of any info ***

- CG can direct its agency to intercept any info transmitted through any computer resource
- The subscriber or intermediary or person in-charge of the computer resource shall extend facilities to decrypt information-
 - o provide access to the computer resource generating, transmitting, receiving or storing info
 - o intercept or monitor or decrypt the info
 - o provide info stored
- Liable if fails to comply

Sec 69A - Powers to issue directions for blocking for public access of any information ***

- CG can direct its agency/intermediary to block any info generated, transmitted, received, stored or hosted in any computer resource
- Procedure & safeguards to be prescribed
- Liable if fails to comply

Sec 69B - Power to authorize to monitor and collect traffic data or information for Cyber Security

- CG to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
- The intermediary or person in-charge shall extend technical assistance and facilities

- Procedure & safeguards to be prescribed
- Liable if fails to comply

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

Sec 70 - Protected system

- The appropriate Government may declare any computer system to be a Critical Information Infrastructure or a protected system. May authorize persons access
- Prescribe the information security practices and procedures
- Liable- Secures access or attempts to secure access

Critical Information Infrastructure- means the computer resource, the incapacitation or destruction of which, shall have devastating impact on national security, economy, public health or safety

Sec 70A - National Nodal Agency

- CG may designate any organization of the Government as the national nodal agency responsible for all measures in respect of Critical Information Infrastructure Protection
- Agency responsible for R&D relating to its protection. Functions and duties as prescribed

Sec 70B - Indian Computer Emergency Response team to serve as national agency for incident response

CG shall appoint an agency. (Director, officers + T&C + salary). Functions and duties as prescribed

Functions in the area of Cyber Security:

- Collection, analysis and dissemination of information on cyber incidents (CI)
- Forecast and alerts of CI
- Emergency measures for handling CI
- Coordination of CI response activities
- Issue guidelines, advisories, vulnerability notes and white papers etc. relating to information security practices & etc. and reporting of CI
- other prescribed functions

Agency may direct service provider, intermediaries, data centers, body corporate or person for info. Liable if fails to do so

Sec 71 - Penalty for misrepresentation

Misrepresentation or suppression any material fact from the Controller or the CA for obtaining any licence or ESC

Sec 72 - Penalty for breach of confidentiality and privacy

Unauthorized (or without consent) disclosure of e-record, book, register, correspondence, information, document etc. to which access is secured pursuant to powers under the Act

Sec 72A - Punishment for disclosure of information in breach of lawful contract

Disclosing material containing personal information about another person which has been secured by a person or intermediary providing services

- o Without the consent of the person with the intent to cause wrongful loss or wrongful gain
- o In breach of a lawful contract

Sec 73 - Penalty for publishing ESC false in certain particulars

No person shall publish a ESC if he knows that-

- CA listed in the certificate has not issued it
- Subscriber listed in the certificate has not accepted it
- Certificate has been revoked or suspended

Sec 74 - Publication for fraudulent purpose

Whoever knowingly creates, publishes or make available a ESC for any fraudulent or unlawful purpose

Sec 75 - Act to apply for offence outside India

- Act shall apply also to any offence or contravention committed outside India by any person of any nationality
- Act shall apply if offence or contravention involves a system located in India

Sec 76 - Confiscation

Any computer system, floppies, compact disks, tape drives or accessories related shall be liable to confiscation (when Act, order, rules contravened)

Sec 77 - Compensation, penalties or confiscation not to interfere with other punishment

No compensation awarded, penalty imposed or confiscation made shall prevent the award of compensation or imposition of other penalty/punishment

Sec 77A - Compounding of Offences

A court of competent jurisdiction may compound offences under this Act. Not be compounded for

- Offences having imprisonment for life or for a term exceeding 3 years
- Accused has previous conviction and is liable to punishment -> either enhanced or different kind
- Offence affects socio-economic conditions or has been committed against a child or a woman

Sec 77B - Offences with 3 years imprisonment to be cognizable_

Offences punishable with imprisonment of 3 years and above shall be cognizable. Rest bailable

Sec 78 - Power to investigate offences

Police officer not below the rank of Inspector shall investigate any offence under this Act

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES [CHAPTER XII]

Sec 79 - Exemption from liability of intermediary in certain cases

- *Network service provider* means an intermediary
- *3rd party information* means any information dealt with by a NSP as an intermediary

An intermediary shall not be liable for any 3rd party information, data, or communication link hosted by him. Apply if Intermediary-

1. Only provides access to the communication system
2. Doesn't 1) initiate the transmission 2) select its receiver 3) select or modify the info
3. Observes due diligence and follow guidelines

Not apply if intermediary-

1. Has conspired or aided by threats or promise etc. in the commission of the unlawful act
2. Fails to remove or disable access to unlawful material of which he has received knowledge, or has been notified by the government

Examiner of Electronic Evidence (CHAPTER XII A)

Sec 79A - Central Government to notify examiner of electronic evidence

CG may specify body/agency to provide expert opinion as an Examiner of e-Evidence

Sec 80 - Power of police officer and other officers to enter search

Any police officer, not below the rank of an Inspector may enter any **public place** (conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public) and **search and arrest without warrant** any person committed or of committing or of being about to commit any offence

Sec 81 - Act to have overriding effect

The provisions of this Act shall have effect notwithstanding anything inconsistent with any other law.
Exception- Copyright Act, Patents Act

Sec 81A - Application of the act to electronic and truncated cheque

The provisions of this act shall apply to, or in relation to e-cheques and the truncated cheques which have the meaning specified in the Negotiable Instruments Act

Sec 82 - Chairperson, members, officers and employees to be public servants

Chairperson, members, officers and employees of the CAT, the Controller, the Deputy and the Assistant Controllers shall be deemed to be Public Servants

Sec 83 - Power to give directions

CG can direct SG as to execute this Act

Sec 84 - Protection of action taken in good faith

No suit or other legal proceeding shall lie against the CG/SG, Controller, Presiding Officer, AO, CAT staff for anything which is done in good faith or in pursuance of the Act

Sec 84A - Modes or methods for encryption

CG may prescribe the modes or methods for encryption

Sec 84B - Punishment for abetment of offences

Whoever abets any offence & if it is committed, shall be punished with the punishment provided for that offence under this Act

Sec 84C - Punishment for abetment of offences

Whoever attempts to commit an or causes such an offence to be committed shall be punished with ____

Sec 85 - Offences by Companies

- Every person who is in-charge (director, manager, sect) or responsible of company shall be guilty
- NA- if offence has taken place without knowledge and exercised all due-diligence. Guilty if done with consent or due to neglect

Sec 86 - Removal of difficulties

Refer book

Sec 87 - Power of CG to make rules

CG may, by notification in the Official Gazette, make rules to carry out the provisions of this Act. Such rules would provide for-

- Modes or methods for encryption
- Conditions for considering reliability of e-signature or e-authentication technique
 - o Procedure for ascertaining e-signature or authentication
 - o Manner in which any information or matter may be authenticated by means of e-signature
- Matters relating to the type of E-Signature, manner and format in which it may be affixed
- Manner of storing and affixing e-signature creation data
- E-form in which filing, issue, grant or payment shall be effected
- Manner and format in which e-records shall be filed or issued and the method of payment
- Period of validity of license granted
- Requirements which an applicant must fulfill
- Form in which an application for license may be made, accompanying documents
- Fees payable, Late fees
- Form and the fee for renewal of a license
- Form of application and fee for issue of ESC
- Duties of subscribers
- Qualifications, experience, salary, allowances and T&C of service of ____
- Manner in which the AO shall hold inquiry
- Procedure for investigation of misbehaviour or incapacity
- Powers and functions of the Chairperson of the CAT
- Manner of performing functions and duties of the agency
- Guidelines to be observed by the intermediaries
- Sensitive personal data or information
- Reasonable security practices and procedures
- Information security practices and procedures for protected system
- Procedures and safeguards for interception, monitoring or decryption
 - o blocking for access by the public
 - o monitoring and collecting traffic data

Sec 88 - Constitution of Advisory Committee

- CG shall constitute a CRAC (Cyber Regulations Advisory Committee)
- 1 Chairperson + official & non-official members
- Committee to advise 1) CG about rules or connected purposes 2) Controller in framing regulations

Sec 89 - Power of controller to make regulations

Consult with CRAC and with approval of CG shall make regulations for the following matters:

- Maintenance of data-base containing the *disclosure record* of every CA
- Conditions and restrictions under which the Controller may recognise any *foreign CA*
- T&C under which a license may be granted to CA
- Other standards to be observed by a CA
- Manner in which the CA shall disclose information
- Particulars of statement which shall accompany an application of a subscriber
- How a subscriber communicates the compromise of private key to the CA

Sec 90 - Power of State Government to make rules

SG may make regulations for the following matters:

- E-form for filing, issue, grant receipt or payment
- Any other matter which is required to be provided by rules by the SG