

CHAPTER 10

INFORMATION TECHNOLOGY (AMENDED) ACT, 2008

HISTORY

- ◆ The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures.
- ◆ The legal recognition to electronic records & digital signatures will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999.
- ◆ In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000.
- ◆ Cyber laws are contained in the Information Technology Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India.

OBJECTIVES:

- ◆ To grant legal recognition for transactions carried out by means of electronic communication (e-commerce) in place of paper based methods of communication,
- ◆ To give legal recognition to digital signature for authentication of any information
- ◆ To facilitate e-filing of documents with government departments
- ◆ To facilitate electronic storage of data
- ◆ To facilitate and give legal sanctions to EFT between banks and financial institutions
- ◆ To give legal recognition for keeping books of accounts by bankers in e-form
- ◆ To amend The Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891 and The RBI Act, 1934.

SCOPE:

- ◆ The act shall extend to whole of India, unless otherwise provided in the Act, it applies to any offence or contravention thereunder committed outside India by any person
- ◆ It shall come into force on such date as the Central Government may notify.

EXCEPTIONS

- ◆ The Act shall not apply to the following:
 - a negotiable instrument as defined in Sec 13 of Negotiable Instruments Act, 1881;
 - a power-of-attorney as defined in Sec 1A of Powers-of-Attorney Act, 1882;
 - a trust as defined in Sec 3 of the Indian Trusts Act, 1882;
 - a will as defined in Sec 2(h) of the Indian Succession Act, 1925;
 - any contract for the sale or conveyance of immovable property or any interest in such property;
 - any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

SECTION 2: DEFINITIONS

(a)	Access	With its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.
(d)	Affixing Electronic Signature	With its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of a Electronic signature.
(f)	Asymmetric Crypto System	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.
(i)	Computer	Any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
(j)	Computer Network	the interconnection of one or more Computers or Computer systems or Communication device through- (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained
(na)	Cyber Café	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.
(nb)	Cyber Security	Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
(o)	Data	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.
(p)	Digital Signature	Authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.
(t)	Electronic Record	Data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

(v)	Information	Includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.
(w)	Intermediary	any particular electronic records, 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.
(x)	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
(zc)	Private Key	The key of a key pair used to create a digital signature.
(zd)	Public Key	The key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate
(ze)	Secure System	Computer hardware, software, and procedure that- i. are reasonably secure from unauthorised access and misuse; ii. provide a reasonable level of reliability and correct operation; iii. are reasonably suited to performing the intended functions; and iv. adhere to generally accepted security procedures

CHAPTER II : DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

AUTHENTICATION OF ELECTRONIC RECORDS USING DIGITAL SIGNATURES (SEC 3)

- ◆ This section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature.
- ◆ Creation of Digital Signature
 - Step 1: The electronic record is converted into a message digest by using a mathematical function known as 'hash function' which digitally freezes the electronic record thus ensuring the integrity of the content of intended communication contained in the electronic record.
 - Step 2: 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 & which can be verified by anybody who has the public key corresponding to the private key.
- ◆ Hash Function

An algorithm mapping or translation of one sequence of bits into another smaller set known as "hash result", such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as it's input making it computationally infeasible-

 - To derive or reconstruct the original electronic record from the hash result produced by the algorithm;
 - That two electronic records can produce the same hash result using the algorithm.

Sec 3A Electronic Signature

A subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered as reliable.

CHAPTER III – ELECTRONIC GOVERNANCE

4	Legal recognition of electronic records	Where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.
5	Legal recognition of Digital Signature	Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of Digital Signature
6	Electronic Governance Foundation	The filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any licence or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.
7	Retention of records in Electronic Form	The documents, records or information retained in the electronic form shall be deemed to have been retained if the same is provided the following conditions are satisfied: (i) the information therein remains accessible so as to be usable subsequently. (ii) The electronic record is retained in its original format or in a format, which accurately represents the information contained. (iii) The details, which will facilitate the identification of the origin, destination, dates and time of despatch or receipt of such electronic record, are available therein.
7A	Audit of Documents etc in Electronic form	Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form
8	Publications in Electronic Gazette	Where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form.
9		The conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central Govt or the State Govt

Section 10: Power to Central Government to make Rules

- ♦ The Central Govt, in respect of Digital Signatures, may prescribe by rules the following:
 - 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.

Sec 10A Validity of contracts formed through electronic means

- Where in a contract formation, the communication of proposals are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

CHAPTER IV: ATTRIBUTION, RECEIPT & DISPATCH OF ELECTRONIC RECORDS

11	This section lays down the manner in which an electronic record is to be attributed to the person who originated it.
12	It provides the manner in which acknowledgement of receipt of an electronic record by various modes is to be made.
13	It provides for the manner in which the time and place of dispatch and receipt of an electronic record sent by the originator shall be identified. Electronic record shall be deemed to be dispatched at the place where the originator has his principal place of business or usual place of residence.

CHAPTER V: SECURE ELECTRONIC RECORDS & SECURE DIGITAL SIGNATURES

14	Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
15	A secure Digital Signature shall be unique to its subscriber, capable of identification the subscriber and exclusive control of subscriber.
16	The power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures.

CHAPTER VI: REGULATION OF CERTIFYING AUTHORITIES

17	Appointment of Controller and other officers to regulate Certifying Authorities.
18	Functions which the Controller may perform in respect of activities of Certifying Authorities.
19	Power of the Controller with previous approval of the Central Government to grant recognition to foreign Certifying Authorities.
20	Omitted vide Information Technology (Amendment) Act 2008

21	Form, fees and other documents to be submitted by a Certifying Authority, to apply for the issue of the license to 'Issue DSC', by the Controller.
22	The application for license shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant and fees not exceeding Rs 25000.
23	The application for renewal of a license (fee not exceeding Rs 5000)
24	The procedure for grant or rejection of license after giving the applicant a reasonable opportunity of being heard.
25	- The Controller may revoke a license, on the grounds such as incorrect or false material particulars being mentioned in the application, contravention of the provisions of the Act, rules, regulation or order issued there under, after giving the applicant a reasonable opportunity of being heard. - No license shall be suspended for a period exceeding 10 days unless the Certifying Authority has been given a chance to present his case.
27	- The Controller may in writing authorize the Deputy Controller, Assistant Controller or any other officer to exercise any of his powers under the Act. Other powers - The Controller shall have the power to investigate contravention of the provisions of the Act either by himself or through any officer authorized in this behalf. - Such person shall have access to any computer system, data or any other material connected with such system if he has reasonable cause to suspect that contravention of the provisions of the Act or rules is being committed.

Duties of Certifying Authorities

- Duties in respect of digital signatures – Sec 30
 - Make use of hardware, software and procedures that are secure from intrusion and misuse,
 - Provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions,
 - Adhere to security procedure to ensure that the secrecy and privacy of the digital signatures are assured, and
 - be the repository of all Electronic Signature Certificates issued under this Act
 - publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and
 - Observe such other standards as may be specified by regulations.
- Ensure that every person employed by him complies with provisions of this Act, or rules, regulations or orders made thereunder – Sec 31
- Display its license at a conspicuous place of the business premises. Surrender the license immediately to the Controller when the same is revoked or suspended – Sec 32 & 33
- Disclose its DSC which contains the public key corresponding to the private key used by that certifying Authority and other relevant facts - Sec 34

CHAPTER VII: ELECTRONIC SIGNATURE CERTIFICATION

Section 35: The procedure for issuance of digital signature certificate.

- ◆ An application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000.
- ◆ Conditions
No DSC shall be granted unless the Certifying Authority is satisfied that:
 - a. The applicant holds the private key corresponding to the public key to be listed in the DSC.
 - b. The applicant holds a private key, which is capable of creating a digital signature,
 - c. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

Suspension: No certificate shall be suspended for a period exceeding 15 days unless the subscriber has been given a reasonable opportunity of being heard. – Sec 37

Section 38: Revocation of DSC by publishing a notice of suspension or revocation of a DSC.

CHAPTER VIII: DUTIES OF SUBSCRIBERS – (SEC 40-42)

- ◆ On acceptance of the DSC the subscriber shall generate a key pair using a secure system.
- ◆ The subscriber shall exercise reasonable care to retain control of his private key corresponding to the public key.
- ◆ If the private key has been compromised the subscriber must immediately communicate the fact to Certifying Authority.

CHAPTER IX: PENALTIES AND ADJUDICATION

Section 43: Penalty for Damage to Computer, Computer System or Network

- ◆ Intruder shall be liable to pay damages by way of compensation *not exceeding Rs. 1 Crore* to the person so affected, for damage to computer, computer system or network by any of the following methods :
 - a. Securing access to computer, computer system or network
 - b. Downloading or extracting any data, computer database or information from such computer system or those stored in any removable storage medium.
 - c. Introducing any computer containment or virus into the computer, computer system or network
 - d. Damaging any computer, computer system or network or any computer data, database or programs
 - e. Disrupting any computer, computer system or network
 - f. Denying access to any person authorized to access the computer, computer system or network
 - g. Providing assistance to any person to access any computer, computer system or network in contravention of any provisions of this Act
 - h. Charging the services availed by one person to the account of another person by tampering with or manipulating any computer, computer system or network

Sec 43A Compensation for failure to protect data

Where a body corporate dealing any sensitive personal data or information in a computer resource which it owns, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, **not exceeding Rs.5 Crores**, to the person so affected.

SECTION 44:

Failure to furnish any document, return or report to the Controller or the Certifying Authority	Penalty not exceeding Rs.1,50,000/- for each such failure
Fails to file any return or furnish any information, books or other documents within the time specified in the regulations	Penalty not exceeding Rs.5,000/- for every day during which such failure continues
Fails to maintain books of account or records	Penalty not exceeding Rs.10,000/- for every day during which the failure continues

Section 45 : Residuary Penalty

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding Rs.25,000/- to the person affected by such contravention or a penalty not exceeding Rs.25,000/-

Section 46: Power to adjudicate contravention under the act to an officer not below the rank of a Director to the Government of India or State Government.

Section 47: While deciding upon the quantum of compensation the adjudicating officer shall have due regard to the amount of gain or unfair advantage and the amount of loss caused to any person as well as the respective nature of the default.

CHAPTER X: CYBER REGULATIONS APPELLATE TRIBUNAL

- ◆ The "Cyber Regulations Appellate Tribunal" has appellate powers in respect of orders passed by any adjudicating officer.
- ◆ Civil courts have been barred from entertaining any suit or proceeding in respect of any matter which an adjudicating officer or Tribunal is empowered to handle.

Section 48: It provides for the

48	Establishment of one or more Appellate Tribunals to be known as "<i>Cyber Regulation Appellate Tribunal</i>" (CRAT) ◆ It shall consist of one person only called the Presiding Officer of the Tribunal and shall be appointed by the Central Government. ◆ The presiding officer shall be a person qualified to be a judge of high court or has been a member of the Indian Legal Service in the post (Grade I) of that service for at least 3 years. ◆ He shall hold office for a term of 5 years or up to the maximum age of 65 years, whichever is earlier.
-----------	---

50	(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court; (2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.
52	Provides for the salary and allowances and other terms and conditions of service of the Presiding Officer.
53	Provides that in the situation of any vacancy occurring in the office of the Presiding Officer, the Central Government shall appoint another person in accordance with the provisions of the Act.
54	Resignation and removal of the Presiding Officer.

APPEAL TO CRAT:

- ◆ An appeal can be made by an aggrieved person against an order of the adjudicating officer to the CRAT.
- ◆ The appeal must be made within 45 days of the receipt of the original order.
- ◆ The Tribunal may accept the appeal after the expiry of 45 days, if it is satisfied that there was sufficient cause for not filing it within the period.
- ◆ No appeal shall be entertained if the original order was passed with the consent of both the parties.

Powers and Procedure of the Appellate Tribunal - Section 58

- ◆ The tribunal shall have the powers of a Civil Court under the Code of Civil Procedure, 1908.
- ◆ It shall have following powers:
 - (a) summoning and enforcing the attendance of any person and examining him on oath;
 - (b) requiring the discovery and production of documents or other electronic records;
 - (c) receiving evidence on affidavits;
 - (d) issuing commissions for the examination of witnesses or documents;
 - (e) reviewing its decisions;
 - (f) dismissing an application for default or deciding it ex parte;
 - (g) any other matter which may be prescribed.

60	Provides for period of limitation for admission of appeals from the aggrieved persons to the Cyber Appellate Tribunal.
61	No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer has jurisdiction to determine
62	Appeal to High Court on question of law or fact arising out of the order of the CRAT within 60 days from the receipt of the order.

63	Any contravention under this Act may be compounded by the Controller or Adjudicating Officer either before or after the institution of adjudicating proceedings subject to such conditions as he may impose. <i>This provision shall not apply to a person who commits the same or similar contravention within a period of 3 years from the date on which the first contravention, committed by him, was compounded.</i>
64	Recovery of penalty as arrears of land revenue and suspension of the license or DSC till penalty is paid.

CHAPTER XI: OFFENCES

Section	Offence	Penalty
65	Tampering computer source	a. Imprisonment up to 3 years, or b. Fine upto Rs.2lakhs, or c. Both.
66	Hacking	a. Imprisonment up to 3 years, or b. Fine upto Rs.5 lakhs, or c. Both
66A	Punishment for sending offensive messages through communication service	Imprisonment for a term upto three years and with fine.
66B	Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment for a term up to three years or with fine up to Rs. 1 lakh or both.
66C	Punishment for identity theft	Imprisonment for a term up to three years or with fine up to Rs. 1 lakh or both.
66D	Punishment for cheating by personation by using computer resource	Imprisonment for a term up to three years or with fine up to Rs. 1 lakh or both.
66E	Punishment for violation of privacy	Imprisonment for a term up to three years or with fine up to Rs. 2 lakh or both.
66F	Punishment for cyber terrorism	Imprisonment which may extend to imprisonment for life

67	Publishing of obscene information in electronic form	First Conviction a. Imprisonment up to 3 years, or b. Fine up to Rs 5 lakh Subsequent Conviction a. Imprisonment up to 5 years, or b. Fine up to Rs 10 lakhs.
67A	Punishment for publishing or transmitting of material containing sexually explicit act, in electronic form	First Conviction a. Imprisonment up to 5 years, or b. Fine up to Rs 10 lakh
67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Subsequent Conviction a. Imprisonment up to 7 years, or b. Fine up to Rs 10 lakhs.
68	Controller's order to cease activities	a. Imprisonment up to 2 years, or b. Fine upto Rs 1lakhs, or c. Both.
69	Controller's order to intercept , monitor or decrypt information	Imprisonment up to 7 years with fine
69A	Directions for blocking for public access of any information through any computer resource	Imprisonment up to 7 years with fine
70	Unauthorized Access of "Protected Systems"	Imprisonment upto 10 years with fine
71	Misrepresenting or suppressing any material fact	a. Imprisonment up to 2 years, or b. Fine upto Rs.1 lakhs, or c. Both
72	Breach of confidentiality	
73	Publishing a false Digital Signature Certificate	
74	Fraudulent Publication	

75	<i>Offence committed outside India</i> Any offence or contravention by a <i>person outside India</i> irrespective of his nationality, shall be punished, if the act or conduct constituting the offence or <i>contravention involves a computer, computer system or computer network located in India.</i>
76	<i>This Section provides for the confiscation of any computer, computer system, floppies, CDs, tape drives or any other accessories related thereto in respect of contravention of any provisions of the Act, rules and regulations or orders made thereunder.</i>
77	<i>The penalty and confiscation provided under this Act shall not interfere with other punishments provided under any other law for the time being in force.</i>
78	Power to investigate the offences under this Act by a police officer not below the rank of Inspector.

CHAPTER XII:**NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES – SECTION 79**

The network service providers (intermediary) shall not be liable to any third party information (information dealt with by the network provider in his capacity as an intermediary) or data made available by him, if he proves that the offence was committed without his knowledge or consent.

CHAPTER XIII: MISCELLANEOUS PROVISIONS**Power of police officer and other officers to enter, search etc - Section 80**

- ◆ Notwithstanding anything contained in Code of Criminal Procedure 1973,
 1. Any police officer not below the rank of Inspector, or
 2. Any other officer of the Central or State Government, if so authorized by Central Govt.

May enter any public place (includes public conveyance, any hotel, any shop or any other place accessible to public) and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or is about to commit any offence under this Act.
- ◆ Where any person is arrested by an officer other than a police officer, such officer shall immediately send the arrested person to
 - i. A magistrate having jurisdiction or
 - ii. The officer in charge of the nearest police station.

Liability of Companies – Section 85

- ◆ Where a company (includes a firm or AOP) commits any offence under this Act, every person, who at the time of contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of such contravention.
 - Such person shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.
- ◆ Where such contravention was committed with the connivance or consent of or due to negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.

Power of Central Government to make rules – Section 87

The Central Government is empowered to make rules in respect of following matters;

- a. The manner in which any matter may be authenticated by a digital signature;
- b. The manner and format in which electronic records shall be filed or issued;
- c. The type of digital signature, manner and format in which It may be affixed;
- d. The security procedure for the purpose of creating same electronic record and secure digital signature;
- e. The qualification, experience and terms and conditions of service of Controller, Deputy Controllers and Asst Controllers;
- f. The requirements manner and form in which application is to be made for license to issue DSC;
- g. The period of validity of the license;
- h. The qualification and experience of an adjudicating officer as well as other officers;
- i. The salary, allowances and terms & conditions of service of the Presiding Officer etc.

Power of State Government to make rules

The State Government is empowered to make rules regarding the following matters:

- The electronic form in which filing, issue, grant, receipt or payment shall be effected in respect of use of electronic records and digital signature in government and its agencies.
- The manner in which such electronic records shall be filled or issued and fee or charges in connection with the same
- Any other matter required to be provided by rules of the State Government

Power of Controller to make regulations - Section 89:

The controller is empowered to make regulations under the Act with the previous approval of Central Government and in consultation with Cyber Regulations Advisory Committee on the following matters:

1. The particulars relating to maintenance of database containing the disclosure record of every Certifying Authority.
2. The conditions and restrictions subject to which the Controller may recognize any Foreign Certifying Authority
3. The terms and conditions subject to which a license may be granted
4. Other standards to be observed by a certifying authority
5. The manner in which the Certifying Authority may make the disclosure u/s 34
6. The particulars of statement to be submitted along with an application for the issue of a DSC.
7. The manner in which the subscriber should communicate the compromise of private key to the Certifying Authority.

श्री
SHANKARA
ACADEMY