Law relating to Information Technology

Lesson 12

KEY CONCEPTS

■ Criminal Intention ■ Search ■ Abetting ■ *Mens Rea* ■ *Actus Reus* ■ Congnizable Offence ■ Non-Congnizable Offence ■ Criminal conspiracy ■ Misappropriation ■ Criminal breach of Trust ■ Accusation ■ Defamation ■ Grievous hurt ■ Attempt ■ Accomplishment ■ Presumption of Innocence ■ Burden of Proof ■ Mutiny ■ Personation

Learning Objectives

To understand:

- Ingredients of Crime and law dealing with the menace of Crime
- Structure of judicial system dealing with criminal cases
- The provisions relating to Bail
- Provisions relating to Compounding of Offences
- Offences relating to the property
- Criminal Breach of Trust
- Offences relating to documents and property marks
- Defamation
- Difference between fine and penalty

Lesson Outline

Information Technology Act, 2000 provides legal framework for electronic governance by giving recognition to electronic records and digital signatures.

The new criminal laws i.e. Bharatiya Nyaya Sanhita 2023, Bharatiya Nagarik Suraksha Sanhita 2023 and Bharatiya Sakshya Adhiniyam 2023 have repealed Indian Penal Code 1860, Criminal Procedure Code 1973 and Indian Evidence Act 1872 (old criminal laws) respectively.

Therefore, by virtue of Section 8 of General Clauses Act 1897, the references to the old criminal laws, unless a different intention appears, be construed as references to the provision of new criminal laws.

REGULATORY FRAMEWORK

- The Information Technology Act, 2000
- Digital Personal Data Protection Act, 2023

INTRODUCTION

"Information technology", most commonly termed as IT is the use of computers or computer system to create, process, store, retrieve, and exchange all kinds of data and information. The term IT is typically used within the context of business operations as opposed to personal or entertainment technologies. An information technology system (IT system) is a communications system, or, more specifically speaking, a computer system — including all hardware, software, and peripheral equipment — operated by a limited group of IT users . United Nations General Assembly by resolution A/RES/51/162, dated the January 30, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce. Subsequent to the adoption of this Resolution, Indian government has passed the Information Technology Act, 2000 on 17th October 2000. Indian Information Technology Act 2000 has tried to adopt legal principles, relating to information technology, enacted earlier by several other countries, as also various guidelines pertaining to information technology law. The Act is supplemented by a number of rules which includes rules for cyber cafes, electronic service delivery, data security, blocking of websites. It also has rules for observance of due diligence by internet intermediaries (ISP's, network service providers, cyber cafes, etc.). Any person affected by data theft, hacking, spreading of viruses can apply for compensation.

With the changing needs and requirement of the information technology and communication, the Information Technology Act 2000 has been substantially amended through the Information Technology (Amendment) Act 2008 which was passed by the Indian Parliament on December 24, 2008 and received the Presidential assent on February 5, 2009. The Amendment Act came into force on October 27, 2009.

The Information Technology Act, 2000, was enacted to make, in the main, three kinds of provisions, as under:

(a) It provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, usually referred to, as "electronic Commerce".

(b) It facilitates the electronic filing of documents with the Government agencies, (and also with the publication of rules etc., in the electronic form).

(c) It amends the, Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934, so as to bring in electronic documentation within the purview of the respective enactments.

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

According to Section 1 (4) of the Information Technology Act, 2000 nothing in Information Technology Act, 2000, shall apply to documents or transactions specified in the First Schedule. The documents or transactions mentioned in first schedule are as under:

1. **Negotiable Instruments with exceptions:** A negotiable instrument (other than a cheque, a Demand Promissory Note or a Bill of Exchange issued in favour of or endorsed by an entity regulated by the Reserve Bank of India, National Housing Bank, Securities and Exchange Board of India, Insurance

Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority) as defined in Section 13 of the Negotiable Instrument Act, 1881.

2. **Power of Attorney with exceptions:** A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 but excluding those power-of-attorney that empower an entity regulated by the Reserve Bank of India, National Housing Bank, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority to act for, on behalf of, and in the name of the person executing them.
3. **Trusts:** A trust as defined in section 3 of the Indian Trust Act, 1882.
4. **Wills:** A will as defined in section 2(h) of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.

DEFINITIONS OF BASIC EXPRESSIONS

Section 2(1) of the Information Technology Act, 2000, contains definitions of various expressions. Some of the definitions are important, for understanding the detailed provisions of the Act and are quoted below:

"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. [Section 2(1)(a)]

"Addressee" means a person who is intended by the originator to receive the electronic record, but does not include any intermediary. [Section 2(1)(b)]

"*Adjudicating Officer*" means an adjudicating officer appointed under sub-section (1) of section 46.

"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 digital signature.[Section 2(1)(d)]

"Appellate Tribunal" means the Appellate Tribunal referred to in sub-section (1) of section 48. [Section 2(1) (da)]

"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. [Section 2(1)(f)]

"Certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing electronic signature Certificates. [Section 2(1) (h)]

"Communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.[Section 2(1) (ha)]

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions, by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. [Section 2(1)(i)]

CASE LAW

Syed Asifuddin and Ors. vs. The State of Andhra Pradesh and Ors. Andhra Pradesh High Court, 2006 (1) ALD Cri 96, 2005 Cri. LJ 4314

In this case it was contended that Insofar as the offence under Section 65 of Information Technology Act is concerned, a telephone handset is not a computer nor a computer system containing a computer programme. Alternatively, in the absence of any law which is in force requiring the maintenance of "computer source code", the allegation that the petitioners concealed, destroyed or altered any computer source code, is devoid of any substance and therefore the offence of hacking is absent.

It was observed by the court that the essential functions in the use of cell phone, which are performed by the MTSO, is the central antenna/central transmitter and other transmitters in other areas well coordinated with the cell phone functions in a fraction of a second. All this is made possible only by a computer, which simultaneously receives, analyses and distributes data by way of sending and receiving radio/electrical signals.

"Computer network" means the interconnection of one or more computers through -

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers, whether or not the interconnection is continuously maintained. [Section 2(1)(j)]

"Computer resource" means computer, computer system, computer network, data, computer database or software. [Section 2(1)(k)]

"Computer system" 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. [Section 2(1)(l)]

"Cyber cafe" 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.[Section 2(1)(na)]

"Cyber security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.[Section 2(1)(nb)]

"Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3. [Section 2(1)(p)]

"Electronic form" with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device. [Section 2(1)(r)]

"Electronic record" means data, recorded or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche. [Section 2(1)(t)]

"Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.[Section 2(1)(ta)]

"Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate.[Section 2(1)(tb)]

"Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche. [Section 2(1)(v)]

"Intermediary" with respect to 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. [Section 2(1)(w)]

"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. [Section 2(1) (x)]

"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, but does not include an intermediary. [Section 2(1)(za)]

"Prescribed" means prescribed by rules made under this Act. [Section 2(1)(zb)]

"Private Key" means the key of a key pair, used to create a digital signature. [Section 2(1)(zc)]

"Public Key" means the key of a key pair, used to verify a digital signature and listed in the Digital Signature Certificate. [Section 2(1)(zd)]

"Secure system" means computer hardware, software, and procedure that–

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures.

"Security Procedure" means the security procedure prescribed under section 16 by the Central Government. [Section 2(1)(zf)]

"Subscriber" means a person in whose name the 1 [electronic signature] Certificate is issued. [Section 2(1)(zf)]

"Verify" in relation to a digital signature, or electronic record or its grammatical variations and cognate expressions, means to determine whether -

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact, or has been altered since such electronic record was so affixed with the digital signature. [Section 2(1)(zh)]

DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

As per section 2(1)(ta) of the Information Technology Act, 2000, "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.

Electronic Signature Certificate are issued under section 35 and includes Digital Signature Certificate and Digital Signature Certificate are issued under section 35 (4) of the Act.

Digital signature (i.e. authentication of an electronic record by a subscriber, by electronic means) is recognised as a valid method of authentication. The authentication is to be effected by the use of "asymmetric crypto system and hash function", which envelop and transform electronic record into another electronic record. [Sections 3(1), 3(2)].

Example

A driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove one's identity, to access information or services on the Internet or to sign certain documents digitally.

Example

Physical documents are signed manually, similarly, electronic documents, for example e-forms are required to be signed digitally using a Digital Signature Certificate.

Verification of the electronic record is done by the use of a public key of the subscriber. [Section 3(3)] The private key and the public key are unique to the subscriber and constitute a functioning "key pair".

Section 3A deals with electronic signature. Section 3A(1) provides that notwithstanding anything contained in section 3(1), but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which—

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

For the purposes of above any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to 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, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfils such other conditions which may be prescribed.

Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

ELECTRONIC GOVERNANCE (LEGAL RECOGNITION OF ELECTRONIC RECORDS)

The Act grants legal recognition to electronic records by laying down that where (by any law) "information" or any other matter is to be in:

(a) writing or

(b) typewritten form or

(c) printed form, then, such requirement is satisfied, if such information or matter is:

  (i) rendered or made available in an electronic form; and

  (ii) accessible, so as to be usable for a subsequent reference. (Section 4)

It may be pointed out that "information", as defined in Section 2(1) (v) of the Act, includes data, text, images, sound, voice, codes, computer programmes, software and data-bases or micro-film or computer-generated "micro-fiche".

Examples of e-governance include Digital India initiative, National Portal of India, Aadhaar Portal, filing and payment of taxes online, digital land management systems, Common Entrance Test etc.

Private transactions

Thus, Section 4 of the Information Technology Act, practically equates electronic record with a manual or typed or printed record. Section 5 deals with legal recognition of electronic signatures. It states that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

It may be noted that "signed", with its grammatical variations and cognate expressions, shall, 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.

Public records

Above provisions are primarily intended for private transactions. The Act then proceeds to bring in the regime of electronic records and electronic signature in public records, by making an analogous provision which grants recognition to electronic records and electronic record signatures, in cases where any law provides for:

(a) the filing of any form, application or any other document with a Governmental office or agency; or

(b) the grant of any licence, permit etc.; or

(c) the receipt or payment of money in a particular manner. (Section 6)

Delivery of services by service provider

According to Section 6A the appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify, by notification in the Official Gazette.

It may be noted that service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

Example

A portal for Ministry of Corporate affairs, MCA 21, has been maintained and operated by Infosys. Earlier it was operated by Tata Consultancy Services. Likewise Income tax portal has also been operated by Infosys. So Infosys is service provider for this purpose.

RETENTION OF INFORMATION

The Act also seeks to permit the retention of information in electronic form, where any law provides that certain documents, records or information shall be retained for any specific period. Certain conditions as to accessibility, format etc. are also laid down. (Section 7)

AUDIT OF DOCUMENTS MAINTAINED 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 the electronic form.(Section 7A)

PUBLICATION OF SUBORDINATE LEGISLATION IN ELECTRONIC GAZETTE

Subordinate legislation is also authorised, by the Act, to be published in the Official Gazette or the electronic Gazette, and the date of its first publication in either of the two Gazette shall be deemed to be the date of publication. (Section 8)

Example

A subordinate legislation was published by the authority in official gazette on 02.01.2020 and in electronic Gazette on 31.12.2019.

The date 31.12.2019 shall be deemed to be the date of publication.

But the provisions summarised above shall not confer any right upon any person to insist, that any Government agency shall accept, issue etc. any document in electronic form or effect any monetary transaction in electronic form. (Section 9)

VALIDITY OF CONTRACTS FORMED THROUGH ELECTRONIC MEANS

The 2008 amendment to the IT Act introduced Sec 10A which provides for a greater acceptance to the electronic contract, establishing without question its validity in the eyes of the law. As more and more businesses and organizations are realizing the effectiveness and efficiency gained by e-commerce, electronic contracts, and e-signatures, we see an increase in legislation supporting it.

As per section 10A of the Act, where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

CASE LAW

The Supreme Court in the 2010 case of *Trimex International FZE Ltd. Dubai vs. Vedanta Aluminium Ltd., India*. ("*Trimex Case*") provided this clarity with regard to contracts concluded on emails. In the Trimex Case the Supreme Court, held that inference can be drawn from documents exchanged on telegram, emails etc. ("Tele communication") that a valid contract subsists given that intention of the party to be bound by the terms of such Tele-communications and essential elements of a valid contract are present.

ATTRIBUTION AND DISPATCH OF ELECTRONIC RECORDS

Since, in an electronic record, the maker remains behind the curtain, it was considered desirable to make a provision for "attribution" of the record. An electronic record is attributed to the "originator". [Defined in Section 2(1)(za)]

Broadly, the "originator" is the person at whose instance it was sent in the following cases -

(a) if it was sent by the originator himself; or

(b) if it was sent by a person authorised to act on behalf of the originator in respect of that electronic record; or

(c) if it was sent by an information system programmed by or on behalf of the originator to operate automatically. (Section 11)

Example

An Automatic email is received from or on behalf of a XYZ Ltd. confirming an order placed in online platform.

This electronic record shall be attributed to the said company.

Regarding acknowledgement of receipt of electronic records, the Act provides that where there is no agreement that the acknowledgment be given in a particular form etc. then the acknowledgement may be given by:

(a) any communication by the addressee (automated or otherwise); or

(b) any conduct of the addressee which is sufficient to indicate to the originator that the electronic record has been received. [Section 12(1)]

Special provisions have been made for cases where the originator has stipulated for receipt of acknowledgment, [Section 12 (b)] or where the acknowledgement is not received by the originator in time. [Section 12(2), 12(3)]

Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall he deemed to have been never sent by the originator.[Section 12(2)]

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent. [Section 12(2)]

These provisions emphasize on the need of acknowledgements for making electronic record binding.

TIME AND PLACE OF DISPATCH ETC.

After these provisions, there follows a provision which is of considerable significance for the law of contracts. The date of offer and the date of acceptance are crucial, in determining whether and which contract has come into existence. The two terminal points - despatch and receipt, are dealt with, in detail. Subject to agreement between the parties, the dispatch of an electronic record occurs, when it enters a "computer resource" outside the control of the originator. [Section 13 (1)]

"Computer resource", as defined in Section 2 (k), means a computer, computer system, computer network, data, computer database or software.

Time of receipt

As regards the time of receipt of electronic records, two situations are dealt with, separately. Subject to agreement, if the addressee has designated a computer resource for receipt, then receipt occurs when the electronic record enters the designated resource. However, if the record is sent to a computer resource of the addressee which is not the designated resource, then receipt occurs at the time when the electronic record is retrieved by the addressee. [Section 13(2)(a)]

If the addressee has not designated a computer resource (with or without specified timings), then receipt is deemed to occur, when the electronic record enters the computer resource of the addressee. [Sections 13(1), 13(2)] Above provisions apply, even where the place of location of the computer is different from the deemed place of receipt.

The Act also contains provisions as to the place of dispatch and receipt. [Section 13(3)]

SECURE ELECTRONIC RECORDS AND SIGNATURES

The Central Government may prescribe the security procedures and practices for the purposes of sections 14 dealing with secure electronic records and 15 dealing with secure electronic signature.

While prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

When the procedure has been applied to an electronic record at a specific point of time, then such record is deemed to be a secure electronic record, from such point of time to the time of verification. (Section 14)

An electronic signature shall be deemed to be a secure electronic signature, if—

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed. (Section 15)

Example

If the signature creation data such as codes or private cryptographic keys are in control of 2 or more persons. The electronic signature cannot be deemed to be a secure electronic signature.

CERTIFYING AUTHORITIES

The Act contains detailed provisions as to "Certifying Authorities" (Sections 17-34). A Certifying Authority is expected to reliably identify persons applying for "signature key certificates", reliably verify their legal capacity and confirm the attribution of a public signature key to an identified physical person by means of a signature key certificate. To regulate the Certifying Authorities, there is a Controller of Certifying Authorities. (Section 17) Obligations of Certifying Authorities are also set out, in the Act. (Sections 30-34)

The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Information Technology Act, 2000. It aims at promoting the growth of E-Commerce and E- Governance through the wide use of digital signatures.

The CCA certifies the public keys of Certifying Authorities (CAs) using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India (RCAI). The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country.

Licenced Certifying Authorities[1]

1. https://cca.gov.in/licensed_ca.html

ELECTRONIC SIGNATURE CERTIFICATES

Sections 35-39 of the Act deal with Electronic Signature Certificates. As per section 35 of the Act, Certifying authority to issue electronic signature Certificate. Followings are the procedure of obtaining electronic signature Certificate:

(1) Any person may make an application in prescribed form to the Certifying Authority for the issue of electronic signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by prescribed fees.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application , the Certifying Authority may, after consideration of the certification practice statement or the other statement and after making such enquiries as it may deem fit, grant the 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 the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Suspension of Digital Signature Certificate (DSC)

The Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,–

(a) on receipt of a request to that effect from–

  (i) the subscriber listed in the Digital Signature Certificate; or

  (ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

A Digital Signature Certificate should not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate, the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate (DSC)

A Certifying Authority may revoke a Digital Signature Certificate issued by it in the following circumstances:

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

Further, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

However, a Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter. On revocation of a Digital Signature Certificate, the Certifying Authority shall communicate the same to the subscriber.

Control of Private Key

Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.

If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

The subscriber is liable till he has informed the Certifying Authority that the private key has been compromised.

PENALTIES AND ADJUDICATIONS

The Act contemplates a dual scheme in regard to wrongful acts concerning computers etc. Certain acts are vested with (so called) "penalties", which are however, adjudicated, not before courts, but before adjudication officers. (Sections 43-47)

In fact, however, though the heading of Section 43 speaks of "penalty and compensation for damage to computer, computer system".

Section 43 provides that if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceal, 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;

he shall be liable to pay damages by way of compensation to the person so affected.

For the purposes of Section 43,–

(i) "Computer contaminant" means any set of computer instructions that are designed–

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network.

(ii) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "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;

(iv) "Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means;

(v) "Computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.

COMPENSATION FOR FAILURE TO PROTECT DATA

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, 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 to the person so affected.(Section 43A)

It may be noted that:

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Penalty for failure to furnish information, return, etc. (Section 44)

If any person who is required under this Act or any rules or regulations made thereunder to–

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding fifteen lakh rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in

the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding fifty thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding one lakh rupees for every day during which the failure continues.

This section has been amended by the Jan Vishwas (Amendment of Provisions) Act, 2023 w.e.f. 30.11.2023.

By way of the amendment, the penalty under this section has now increased to 10 times of penalties provided before the amendment.

Residuary Penalty (Section 45)

Whoever contravenes any rules, regulations, directions or orders made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a penalty not exceeding one lakh rupees, in addition to compensation to the person affected by such contravention not exceeding—

(a) ten lakh rupees, by an intermediary, company or body corporate; or

(b) one lakh rupees, by any other person.

This section has been amended by the Jan Vishwas (Amendment of Provisions) Act, 2023 w.e.f. 30.11.2023.

By way of the amendment, the penalty has now increased from INR 25,000 to INR 1,00,000, and compensation (which was earlier an alternative to the penalty) has also been extended to (i) INR 10,00,000 for a contravention by an intermediary, company or body corporate, or (ii) INR 1,00,000 for a contravention by a person.

Power to adjudicate (Section 46)

According to section 46(1), for the purpose of adjudging under this Act whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of section 46(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

The adjudicating officer appointed under section 46(1) can exercise jurisdiction to adjudicate matters in which the claim for damage does not exceed rupees five crore and the jurisdiction in respect of the claim for damage exceeding rupees five crores is vested with the competent court.

Adjudicatory Process: According to section 46(2), the adjudicating officer can, after giving the person referred to in section 46(1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

Qualification for Adjudicating Officer: According to section 46(3), no person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

Powers of Adjudicating Officer: Every adjudicating officer shall have the powers of a civil court which are conferred on the Appellate Tribunal under section 58(2), and–

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973;

(c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.

This section has been amended by the Jan Vishwas (Amendment of Provisions) Act, 2023 w.e.f. 30.11.2023.

By way of the amendment, the scope of adjudication through a central government appointed officer under section 46 has also been expanded to the entire Act. Earlier, it was restricted to Chapter IX of the Act, that is, the chapter related to penalties, compensation, and adjudication.

CYBER REGULATION APPELLATE TRIBUNAL

Chapter X of the Act provides for the establishment of Appellate Tribunal. (Sections 48-62). The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997 , shall, on and from the commencement of Part XIV of Chapter VI of the Finance Act, 2017 (7 of 2017), be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act.

The Central Government shall specify, by notification the matters and places in relation to which the Appellate Tribunal may exercise jurisdiction.

In the same Chapter, there are provisions regarding the compounding of offences and recovery of penalties. (Sections 63 and 64).

Any person aggrieved by an order of the Controller of Certifying Authorities or of the adjudicator can appeal to the Appellate Tribunal, within 45 days. (Section 57)

Any person aggrieved by “any decision or order” of the Appellate Tribunal may appeal to the High Court, within 60 days. Jurisdiction of Civil Courts is barred, in respect of any matter which an adjudicating officer or the Appellate Tribunal has power to determine.

OFFENCES

Chapter XI of the Act, (Sections 65-78) deals with offences relating to computers etc. and connected matters.

Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

It may be noted that “computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.(Section 65)

Computer related offences

If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. (Section 66)

The offences listed in the Act are the following –

- Dishonestly receiving stolen computer resource or communication device
- Identity theft
- Cheating by personation by using computer resource

- Violation of privacy
- Cyber terrorism
- Publishing or transmitting of material containing sexually explicit act, etc., in electronic form
- Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form
- Misrepresentation
- Breach of confidentiality and privacy
- Disclosure of information in breach of lawful contract
- Publishing electronic signature Certificate false in certain particulars
- Publication for fraudulent purpose.

Chapter XI of the I T Act also contains certain provisions empowering the Controller of Certifying Authorities to issue certain directions to certifying Authorities (Section 68).

Before the Amendment, any person who intentionally or knowingly fails to comply with any order under section 68(1) were liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.

However, after the enactment of the Jan Vishwas (Amendment of Provisions) Act, 2023, any person who intentionally or knowingly fails to comply with any order under section 68(1) are guilty of an offence and are liable to penalty which may extend to twenty-five lakh rupees.

The quantum of fine has been increased substantially and punishment relating to Imprisonment has now been done away with.

Further, as per section 69 where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do , in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of safeguard and procedure as may be prescribed , for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

CASE STUDY

Shreya Singhal v. Union of India (2015) 5 SCC 1

In this case, petitions were filed arguing that Section 66A of the Information Technology Act of 2000 raises very important and far-reaching questions relating primarily to the was violation of fundamental right of free speech and expression guaranteed by Article 19(1)(a) and Right to Equality under Article 14 of the Constitution of India. Court observed that:

"Information that may be grossly offensive or which causes annoyance or inconvenience are undefined terms which take into the net a very large amount of protected and innocent speech....

We have already held that Section 66A creates an offence which is vague and overbroad, and, therefore, unconstitutional under Article 19(1)(a) and not saved by Article 19(2). We have also held that the wider range of circulation over the internet cannot restrict the content of the right under Article 19(1)(a) nor can it justify its denial.....

We find, therefore, that the challenge on the ground of Article 14 must fail... Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2)."

Section 66A of the Information Technology Act, 2000 which penalised people for sending "offensive" messages through any communication services, has also now formally been removed from the Act through the Jan Vishwas (Amendment of Provisions) Act, 2023.

Extraterritorial operation

Extra-territorial operation of the Act is provided for, by enacting that the provisions of the Act apply to any offence or contravention committed outside India by any person, irrespective of his nationality, if the act or conduct in question involves a computer, computer system or computer network located in India. (Section 75)

EXEMPTION FROM LIABILITY OF INTERMEDIARY IN CERTAIN CASES

According to section 79(1) of the Act, an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. However, this provision is subject to section 79 (2) & (3) of the Act provided below.

According to section 79(2), the provisions of sub-section (1) shall apply if:

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not:

  (i) initiate the transmission,

  (ii) select the receiver of the transmission, and

  (iii) select or modify the information contained in the transmission.

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

According to section 79(3) The provisions of sub-section (1) shall not apply if:

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

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

In this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

Data privacy and protection in today's world has become a matter of Individual rights. The right to privacy is recognized as a fundamental right under Article 21 of the Indian constitution which was held in the historic verdict by the Supreme Court in the case of Justice KS Puttaswamy v. Union of India. India's digital transformation requires the law to transform as well. Information Technology Act, 2000 ('the IT Act') and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, commonly known as SPDI Rules, is one of the key legislations in this area.

Under Section 87(2) read with Section 43 – A of the IT Act, "SPDI Rules" were issued on 13th of April 2011 which govern the Sensitive Personal Data or information and apply to body corporate or any person located in India.

The rules define sensitive personal data under the Rule 3 that the following types of data or information shall be considered as personal and sensitive:

- Passwords,
- Bank Account details,
- Credit/debit card details,
- Present and past health records,
- Sexual orientation,
- Biometric data

An information provider is a person who provides information to the body corporate and under these rules, he has certain rights over the sensitive personal information, this information cannot be collected without the providers' consent and he or she has the right to abstain from giving consent and can withdraw the consent by writing to the body corporate.

i. **Privacy Policy**

Rule 4 requires a body corporate to provide a privacy policy on their website, which is easily accessible, provides for the type and purpose of personal, sensitive personal information collected and used, and Reasonable security practices and procedures.

ii. **Consent**

Rule 5 requires that prior to the collection of sensitive personal data, the body corporate must obtain consent, either in writing or through fax regarding the purpose of usage before collection of such information.

iii. **Collection Limitation**

Rule 5 (2) requires that a body corporate should only collect sensitive personal data if it is connected to a lawful purpose and is considered necessary for that purpose.

iv. **Notice**

Rule 5(3) requires that while collecting information directly from an individual, the body corporate must provide the following information:

- The fact that information is being collected
- The purpose for which the information is being collected
- The intended recipients of the information
- The name and address of the agency that is collecting the information
- The name and address of the agency that will retain the information

v. **Retention Limitation**

Rule 5(4) requires that body corporate must retain sensitive personal data only for as long as it takes to fulfil the stated purpose or otherwise required under law.

vi. **Purpose**

Limitation Rule 5(5) requires that information must be used for the purpose that it was collected for.

vii. Right to Access and Correct

Rule 5(6) requires a body corporate to provide individuals with the ability to review the information they have provided and access and correct their personal or sensitive personal information.

viii. Right to 'Opt Out' and Withdraw Consent

Rule 5(7) requires that the individual must be provided with the option of 'opting out' of providing data or information sought by the body corporate. Also, they must have the right to withdraw consent at any point of time.

ix. Grievance Officer

Rule 5(9) requires that body corporate must designate a grievance officer for redressal of grievances, details of which must be posted on the body corporate's website and grievances must be addressed within a month of receipt.

x. Disclosure with Consent, Prohibition on Publishing and Further Disclosure

Rule 6 requires that body corporate must have consent before disclosing sensitive personal data to any third person or party, except in the case with Government agencies for the purpose of verification of identity, prevention, detection, investigation, on receipt of a written request. Also, the body corporate or any person on its behalf shall not publish the sensitive personal information and the third party receiving the sensitive personal information from body corporate or any person on its behalf shall not disclose it further.

xi. Requirements for Transfer of Sensitive Personal Data

Rule 7 requires that body corporate may transfer sensitive personal data into another jurisdiction only if the country ensures the same level of protection and may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

xii. Security of Information

Rule 8 requires that the body corporate must secure information in accordance with the ISO 27001 standard or any other best practices notified by Central Government, which must be audited annually or when the body corporate undertakes a significant up gradation of its process and computer resource.

LAW OF PERSONAL DATA PROTECTION

Digital Personal Data Protection Act, 2023 got the assent of the Hon'ble President of India on 11th August, 2023. The law creates a full framework for the protection of digital personal data in India. It explains what organisations must do when they collect or use such data.

The purpose of this law is to provide the law relating to the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

The Act follows the SARAL approach. This means it is Simple, Accessible, Rational and Actionable. Further, the Government of India has also notified the **Digital Personal Data Protection (DPDP) Rules, 2025** on 14th November 2025. This marks the operationalisation of the **Digital Personal Data Protection Act, 2023 (DPDP Act)**.

Together, the Act and the Rules form a clear and citizen-centred framework for the responsible use of digital personal data. They place equal weight on individual rights and lawful data processing.

In addition to the objectives outlined under the Act, the Digital Personal Data Protection Rules, 2025 operationalise the Act by prescribing practical obligations for Data Fiduciaries, timelines for compliance, formats for notices, consent requirements, processing conditions, security safeguards, and detailed procedures for breach notification.

Following the notification of the DPDP Rules, 2025, the Digital Personal Data Protection (DPDP) Act, 2023, is being implemented in a three-phase, 18-month rollout. The DPDP Rules provide an 18-month phased compliance timeline, allowing organisations time for smooth transition. They also require Data Fiduciaries to issue standalone, clear and simple consent notices that transparently explain the specific purpose for which personal data is being collected and used. Consent Managers—entities that help individuals manage their permissions—must be Indian companies. Phases and their corresponding timelines are as follows:

Phase 1: Immediate Effect (November 13, 2025)

This phase focuses on the institutional and foundational legal framework. Key provisions that are now active include the establishment of the Data Protection Board of India (DPBI) and its operational procedures, definitions within the Act and Rules, and the government's rule-making powers. The regulator is now operational.

Phase 2: After One Year (November 12, 2026)

This intermediate phase is dedicated to the Consent Manager ecosystem. Provisions relating to the registration and obligations of Consent Managers will come into force, allowing these entities time to meet the required standards and register with the DPBI.

Phase 3: After Eighteen Months (May 12, 2027)

The final phase activates the majority of the core operational compliance obligations for all Data Fiduciaries. This is the time limit for businesses to implement comprehensive changes across their systems. Key requirements effective from this date include:

- Mandatory notice and consent mechanisms.
- Implementing security safeguards and data breach notification procedures.
- Processing personal data of children with verifiable parental consent.
- Establishing systems for Data Principal rights (access, correction, erasure) and grievance redressal.
- Adhering to data retention and automated erasure requirements.
- Complying with additional obligations for Significant Data Fiduciaries (e.g., Data Protection Impact Assessments, audits).

Important Definitions under the DPDP Act, 2023

- "Board" means the Data Protection Board of India established by the Central Government.

  Under Rules 14 to 17 of the DPDP Rules 2025, the Board is constituted as a 'Digital-First Adjudicatory Body'. All filings, notices, hearings, replies, and orders will occur through an online portal to ensure speed and transparency. The Board will consist of four Members and will function entirely through digital mechanisms for inquiry, adjudication, and grievance redressal. Appeals from the Board's orders shall lie before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

- "Data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.

- "Data Principal" means the individual to whom the personal data relates and where such individual is—
  - (i) a child, includes the parents or lawful guardian of such a child;
  - (ii) a person with disability, includes her lawful guardian, acting on her behalf.
- "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary.
- "Personal data" means any data about an individual who is identifiable by or I n relation to such data;
- "Personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;
- "Processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;
- "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data; and "person" includes—
  - (i) an individual;
  - (ii) a Hindu undivided family;
  - (iii) a company;
  - (iv) a firm;
  - (v) an association of persons or a body of individuals, whether incorporated or not; (vi) the State; and
  - (vii) every artificial juristic person, not falling within any of the preceding sub-clauses.
- **Consent Manager:** An entity that provides a single, transparent and interoperable platform through which a Data Principal may give, manage, review or withdraw consent.
- **Appellate Tribunal:** The Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which hears appeals against decisions of the Data Protection Board.

Application of the Act

According to section 3, subject to the provisions of this Act, it shall-

(a) apply to the processing of digital personal data within the territory of India where the personal data is collected–
  - (i) in digital form; or
  - (ii) in non-digital form and digitised subsequently;

(b) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

(c) not apply to—
  - (i) personal data processed by an individual for any personal or domestic purpose; and

(ii) personal data that is made or caused to be made publicly available by—

(A) the Data Principal to whom such personal data relates; or

(B) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Rule 4 of the DPDP Rules 2025 introduces a phased compliance schedule extending up to eighteen months from the date of notification of the Rules. During this period, Data Fiduciaries may progressively implement consent mechanisms, breach reporting systems, data retention policies, and user rights redressal systems. Full compliance becomes mandatory for all Data Fiduciaries upon completion of the eighteen-month window.

Rule 12 provides operational clarity for exempted categories by requiring Data Fiduciaries to maintain limited logs even in respect of data categories that are partially exempt or processed for domestic purposes. Government-notified exemptions under the Act must comply with proportionality safeguards, and the processing must remain consistent with the principles of purpose limitation and data minimisation.

LESSON ROUND-UP

- The Information Technology Act has been passed to give effect to the UN resolution and to promote efficient delivery of Government services by means of reliable electronic records. The Act came into effect on 17.10.2000.
- The purpose of the Act is (a) to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as"electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and (b) to facilitate electronic filing of documents with the Government agencies.
- Any subscriber may authenticate an electronic record by affixing his electronic signature.
- "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the Act.
- The digital signature will be certified by 'Certifying Authority'. The 'certified authority' will be licensed, supervised and controlled by 'Controller of Certifying Authorities'.
- The Act contemplates a dual scheme in regard to wrongful acts concerning computers, etc. Certain acts are visited with (so called) "penalties", which are however, adjudicated, not before courts, but before adjudication officers.
- The Act provides for the establishment of one or more Appellate Tribunal and lays down various provisions regarding its jurisdiction, composition, powers and procedure.
- Any person aggrieved by an order of the Controller of Certifying Authorities or of the adjudicator can appeal to the Appellate Tribunal.
- Chapter XI of the Act spells out provisions regarding offences relating to computers, etc. This chapter also contains provisions empowering the Controller of Certifying Authorities to issue certain directions to Certifying Authorities and to subscribers. There is also a provision for confiscation.

- A committee led by former Supreme Court Justice B.N. Srikrishna, constituted in August 2017, submitted the draft Personal Data Protection(PDP) Bill 2018. But, the bill that was designed to protect the privacy of Indians, the Personal Data Protection Bill 2019, was withdrawn by the government with an assurance that a new bill will soon be tabled.

GLOSSARY

Affixing electronic Signature: 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 digital signature.

Biometrics : Biometrics means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes.

Cyber incidents: Cyber incidents means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation.

Cyber Security: Cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Electronic Record: Electronic 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.

Electronic Signature: Electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.

TEST YOURSELF

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. Summaries the main provisions contained in the Information Technology Act, 2000.
2. What is the significance of electronic records under the Information Technology Act, 2000?
3. State very briefly the gist of the concepts of "computer network", "electronic form" and "key pair", under the Information Technology Act, 2000.
4. What are the offences provided in the Information Technology Act, 2000, for various kinds of misuse of computer?
5. State, in brief, about the Appellate Tribunal, under the Information Technology Act, 2000.
6. Enumerate the offences punishable under section 66 of Information Technology Act, 2000.

LIST OF FURTHER READINGS
• Bare Act of the Information Technology Act, 2000 • Articles by the professionals and Firms • Kamath Nandan, Law Relating to Computers Internet & E-commerce - A Guide to Cyber laws & The Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws (2012) • Karnika Seth, Computers Internet and New Technology Laws (2013) • Law of Information Technology (Cyber Law) — D.P. Mittal.

OTHER REFERENCES (INCLUDING WEBSITES / VIDEO LINKS)
• https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf