Information Technology Act 2000

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper-based methods of communication and storage of information.

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft.

After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber-crime and to facilitate speedy locating of a cybercriminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. Finally, this suggestion was dropped by the IT Ministry in its final draft.

The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.

With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000.

This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

Background

The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000. The bill was finalised by a group of officials headed by the then Minister of Information Technology, Pramod Mahajan.

Preliminary

1. Short title, extent, commencement and application

- This Act may be called the Information Technology Act, 2000.
- It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also 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, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.
- Nothing in this Act shall apply to -
  - a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881.
  - a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882.
  - a trust as defined in section 3 of the Indian Trusts Act, 1882.
  - a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
  - 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.

Definitions

(1) In this Act, unless the context otherwise requires,

(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;

(b) “Addressee” means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) “Adjudicating Officer” means adjudicating officer appointed under subsection (1) of section 46;

(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 Electronic Signature;

(e) “Appropriate Government” means as respects any matter:

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) “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;

(g) “Certifying Authority” means a person who has been granted a licence to issue a Electronic Signature Certificate under section 24;

(h) “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;

(ha) “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.

(i) “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;

(j) “Computer Network” means 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;

(k) “Computer Resource” means computer, communication device, computer system, computer network, data, computer database or software;

(l) “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;

(m) “Controller” means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;

(n) “Cyber Appellate Tribunal” means the Cyber Appellate Tribunal established under sub-section (1) of section 48;

(na) “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.

(nb) “Cyber Security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored threin from unauthorized access, use, disclosure, disruption, modification or destruction.

(o) “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a 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” 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;

(q) “Digital Signature Certificate” means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) “Electronic Form” with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) “Electronic Gazette” means official Gazette published in the electronic form;

(t) “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;

(ta) “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

(tb) “Electronic Signature Certificate” means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate”

(u) “Function”, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) “Indian Computer Emergency Response team” means an agency established under sub-section (1) of section 70 B

(v) “Information” includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer-generated micro fiche;

(w) “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;

(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;

(y) “Law” includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President’s Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) “Licence” means a licence granted to a Certifying Authority under section 24;

(za) “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;

(zb) “Prescribed” means prescribed by rules made under this Act;

(zc) “Private Key” means the key of a key pair used to create a digital signature;

(zd) “Public Key” means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) “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;

(zf) “Security Procedure” means the security procedure prescribed under section 16 by the Central Government;

(zg) “Subscriber” means a person in whose name the Electronic Signature Certificate is issued;

(zh) “Verify” in relation to a digital signature, electronic record or public key, with 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.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

Amendments

A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". Additionally, it introduced provisions addressing: pornography, child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day, it was passed by the Rajya Sabha. It was signed into law by the then President Pratibha Patil, on 5 February 2009.

Future changes

On 2 April 2015, the then Chief Minister of Maharashtra, Devendra Fadnavis revealed to the state assembly that a new law was being framed to replace the repealed Section 66A. Fadnavis was replying to a query by Shiv Sena leader Neelam Gorhe. Gorhe had said that the repeal of the law would encourage online miscreants and asked whether the state government would frame a law in this regard. Fadnavis said that the previous law had resulted in no convictions, so the law would be framed such that it would be strong and result in convictions.

On 13 April 2015, it was announced that the Ministry of Home Affairs would form a committee of officials from the Intelligence Bureau, Central Bureau of Investigation, National Investigation Agency, Delhi Police and the ministry itself to produce a new legal framework. This step was reportedly taken after complaints from intelligence agencies that they were no longer able to counter online posts that involved national security matter or incited people to commit an offence, such as online recruitment for ISIS. Former Minister of State with the Ministry of Information Technology, Milind Deora has supported a new "unambiguous section to replace 66A".

In 2022, it was reported that there has been a proposal to replace the Information Technology Act with a more comprehensive and updated Digital India Act, which would cover a wider range of information technology issues and concerns. This law could ostensibly have focal areas around privacy, social media regulation, regulation of over-the-top platforms, internet intermediaries, introducing additional contraventions or offences, and governance of new technologies.

Authentication of Electronic Records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation –

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

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

(b) accessible so as to be usable for a subsequent reference

Legal recognition of Electronic Signature

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should 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.

Explanation –

For the purposes of this section, “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.

Attribution of Electronic Records

An electronic record shall be attributed to the originator

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

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgement of Receipt

(1) Where the originator has not stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by –

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

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) 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 be deemed to have been never sent by the originator.

(3) 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 acknowledgment 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.

Time and place of despatch and receipt of electronic record

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely –

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to "be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section –

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

Regulation Of Certifying Authorities

Appointment of Controller and other officers

1. The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers, other officers and employees as it deems fit.
2. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
3. The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
4. The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees shall be such as may be prescribed by the Central Government.
5. The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
6. There shall be a seal of the Office of the Controller.

The Controller may perform all or any of the following functions, namely –

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;

(g) specifying the form and content of a Electronic Signature Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Recognition of foreign Certifying Authorities

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

License to issue electronic signature certificates

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Electronic Signature Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this section shall –

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

Application for licence

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government .

(2) Every application for issue of a licence shall be accompanied by-

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

Renewal of licence

An application for renewal of a licence shall be –

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence:

Procedure for grant or rejection of licence

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application:

Provided that

no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Suspension of Licence

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has –

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the standards specified in Section 30

(d) contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the license:

Provided that

no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any enquiry ordered by him:

Provided that

no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

Notice of suspension or revocation of licence

(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data-base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

Provided that

the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock

Provided further

that the Controller may, if he considers necessary, publicise the contents of the data-base in such electronic or other media, as he may consider appropriate.

Power to delegate

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

Power to investigate contraventions

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

Access to computers and data

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.

Certifying Authority to follow certain procedures

Every Certifying Authority shall-

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which arc reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured;

(ca) be the repositiry of all Electronic Signature Certificates issued under this Act;

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certifcates; and

(d) observe such other standards as may be specified by regulations.

Certifying Authority to ensure compliance of the Act, etc

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

Display of licence

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

Surrender of licence

(1) Every Cerifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(2) Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offense and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

Disclosure

(1) Every Certifying Authority shall disclose in the manner specified by regulations

(a) its Electronic Signature Certificate

(b) any certification practice statement relevant thereto;

(c) notice of revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall-

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Secure Electronic Record

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.

Secure Electronic Signature

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

Explanation- In case of digital signature, the "signature creation data" means the private key of the subscriber.

Security procedures and Practices

The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices

Provided that in 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.

DUTIES OF SUBSCRIBERS

Generating Key Pair

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, (*) the subscriber shall generate that key pair by applying the security procedure.

Duties of subscriber of Electronic Signature Certificate

In respect of Electronic Signature Certificate, the subscriber shall perform such duties as may be prescribed.

Acceptance of Digital Signature Certificate

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate –

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Control of Private key

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

(2) 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.

Explanation – For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Penalty and Compensation for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is incharge 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 injurously by any means;

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

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

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.

Penalty for failure to furnish information, return, etc

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 one lakh and fifty thousand 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 therefore in the regulations, he shall be liable to a penalty not exceeding five 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 ten thousand rupees for every day during which the failure continues.

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 twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Offences

Section 65: 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.

Explanation –

For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Section 66: 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.

Explanation: For the purpose of this section, -

a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

Section 66A: Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C: Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D: Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E: Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section–

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66F: Punishment for cyber terrorism

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an

offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Section 67: Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science,literature,art,or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Section 67 C: Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Section 68: Power of Controller to give directions

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

Section 69: Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense 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 sub-section (2), 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 transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 69A: Power to issue directions for blocking for public access of any information through any computer resource

(1) Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense 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, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

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

Section 70: Protected system

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Section 70 A: National nodal agency

(1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

Section 70 B: Indian Computer Emergency Response Team to serve as national agency for incident response

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security, -

(a) collection, analysis and dissemination of information on cyber incidents

(b) forecast and alerts of cyber security incidents

(c) emergency measures for handling cyber security incidents

(d) Coordination of cyber incidents response activities

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

(f) such other functions relating to cyber security as may be prescribed

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6) , shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).

Section 71: Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72: Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72 A: Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Section 73: Penalty for publishing electronic Signature Certificate false in certain particulars

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74: Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 75: Act to apply for offence or contraventions committed outside India

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 76: Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that

where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Section 77: Compensation, penalties or confiscation not to interfere with other punishment

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

Section 77A: Compounding of Offences

(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Section 77B: Offences with three years imprisonment to be cognizable

(1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Section 78: Power to investigate offences

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any cognizable offence under this Act.

(2)When information is given to an officer in charge of a police station of the commission within the limits of such station of a non-cognizable offence under this act, he shall cause to be entered the substance of the information in a book to be kept by such officer in such form as the State Government may prescribe in this behalf.

(3) Any Police officer receiving such information may exercise the same powers in respect of investigation (except the power to arrest without warrant) as an officer in charge of the police station may exercise in a cognizable case under section 156 of the Code of Criminal Procedure, 1973.