A. **INTRODUCTION: NEED FOR ENACTMENT OF INFORMATION TECHNOLOGY ACT, 2000**

In the knowledge society of 21st century, computer, internet and ICT or e-revolution has changed the lifestyle of the people. Today paper based communication has been substituted by e-communication, paper based commerce by e-commerce and paper based governance by e-governance. Accordingly we have new terminologies like cyber world, netizens, e-transaction, e-banking, e-return and e-contracts. Apart from positive side of e-revolution there is seamy side also as computer; internet and ICT in the hands of criminals has become weapon of offence. Accordingly a new branch of jurisprudence emerged to tackle the problems of cyber crimes in cyber space i.e. Cyber Law or Cyber Space Law or Information Technology Law or Internet Law.¹

For the first time, a Model Law on E-commerce was adopted in 1996 by United Nations Commission on International Trade and Law (UNCITRAL). It was further adopted by the General Assembly of the United Nations by passing a resolution on 31st January, 1997. Further, India was also a signatory to this Model Law and had to revise its national laws as per the said model law. Therefore, India enacted the Information Technology Act, 2000 and it was recently amended by the Information Technology (Amendment) Act, 2008.

1. **National reasons**

   Following are the main national reasons for the enactment of the IT Act, 2000:

   i. Increasing use of ICTs in conducting business transactions and entering into contracts, because it was easier, faster and cheaper to store, transact and communicate electronic information than the traditional paper documents.

   ii. Business people were aware of these advantages but were reluctant to interact electronically because there was no legal protection under the existing laws.

2. **International reasons**

   Following are the main international reasons for the enactment of the IT Act, 2000:

---

i. International trade through electronic means was growing tremendously and many countries had switched over from traditional paper based commerce to e-commerce.

ii. The United Nations Commission on International Trade Law (UNCITRAL) had adopted a Model Law on Electronic Commerce in 1996, so as to bring uniformity in laws governing e-commerce across the globe.

iii. India, being a signatory to UNCITRAL, had to revise its national laws as per the said model law. Therefore, India also enacted the IT Act, 2000.

iv. Because the World Trade Organization (WTO) was also likely to conduct its transactions only in electronic medium in future.

B. **AIMS AND OBJECTIVES OF INFORMATION TECHNOLOGY ACT, 2000**

Following were the main aims and objectives\(^2\) of the IT Act, 2000:

1. To suitably amend existing laws in India to facilitate e-commerce.

2. To provide legal recognition of electronic records and digital signatures.

3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.

4. To provide legal recognition to business contacts and creation of rights and obligations through electronic media.

5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.

6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.

7. To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.

8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various

---

provisions which deal with offences relating to documents and paper based transactions.

9. To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.

10. To amend the Banker’s Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.


C. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

1. Digital Signatures

Basically digital signature is a secure method of binding the identity of the signer with electronic record or message. This method uses a public key crypto system commonly known as ‘asymmetric crypto system’ to generate digital signature.3

i. Definition of Digital Signature

Digital signature means ‘authentication of any electronic record by a subscriber by means of an electronic method or procedure’.

ii. Functions of digital signature

Following are the main functions of digital signature

a. To provide authenticity, integrity, secrecy and non-repudiation to electronic record or message.

b. To use the internet as a safe and secure medium without any violation or compromise for any e-transaction.

iii. Legal provision relating to digital signature

The IT Act, 2000 contains following provisions relating to digital signature:

a. Authentication of electronic records

Any subscriber may authenticate an electronic record by affixing his digital signature.5

---

4 The Information Technology Act, 2000; Section 2 (1) (p)
b. **Authentication by use of asymmetric crypto system and hash function**

The authentication of 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.\(^6\)

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:

- To derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- That two electronic records can produce the same hash result using the algorithm.\(^7\)

c. **Verification of electronic record**

Any person by the use of public key of the subscriber can verify the electronic record.\(^8\)

d. **Private key and public key are unique**

The private key and the public key are unique to the subscriber and constitute a functioning key pair.\(^9\)

2. **Electronic Signature**

Electronic signature is a wide term and it refers to various methods by which one can sign an electronic record. Electronic signature is a technology neutral term and may take many forms and could be created by different technologies.

i. **Definition of electronic signature**

Electronic signature means authentication of any electronic record by a subscriber by means of an electronic technique.\(^10\)

ii. **Legal provisions relating to electronic signature**

The IT Act contains following provisions relating to electronic signature:

---

\(^5\) *Ibid.*, Section 3 (1)
\(^6\) *Ibid.*, Section 3 (2)
\(^7\) *Ibid.*, Explanation to Section 3 (2)
\(^8\) *Ibid.*, Section 3(3)
\(^9\) *Ibid.*, Section 3 (4)
\(^10\) *Ibid.*, Section 2 (1) (ta)
a. **Authentication of electronic record by electronic signature**

A subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable.\textsuperscript{11}

b. **Reliable electronic signature or electronic authentication technique**

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

- The signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or the authenticator and to no other person;
- The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or the authenticator and of no other person;
- Any alteration to the electronic signature made after affixing such signature is detectable;
- Any alteration to the information made after its authentication by electronic signature is detectable; and
- It fulfils such other conditions which may be prescribed.\textsuperscript{12}

c. **Verification of electronic signature**

The 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.\textsuperscript{13}

3. **Secure electronic records and secure electronic signatures**

i. **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 secure electronic record from such point of time to the time of verification.\textsuperscript{14}

ii. **Secure electronic signature**

An electronic signature shall be deemed to be secure electronic signature if –

\textsuperscript{\begin{tabular}{l}
11 \textit{Ibid.}, Section 3A (1) \\
12 \textit{Ibid.}, Section 3A (2) \\
13 \textit{Ibid.}, Section 3A (3) \\
14 \textit{Ibid.}, Section 14
\end{tabular}}
a. The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
b. The signature creation data was stored and affixed in such exclusive manner as may be prescribed.\textsuperscript{15}

iii. Security procedures and practices

The Central Government may prescribe security procedures and practices for secure electronic record and secure electronic signature.\textsuperscript{16} However, for this purpose, the Central Government shall take into account the commercial circumstances, nature of transaction and other related factors as it considers appropriate.\textsuperscript{17}

D. ELECTRONIC GOVERNANCE

Computers, internet and ICTs have various advantages and had brought tremendous change in our lives. Today we have various new concepts like e-contract, e-communication, e-transaction, e-governance and so on.

1. Meaning of E-governance

E-governance is the application of ICTs to the processes of government functioning so as to have simple, accountable, speedy, responsive and transparent governance. Further, the World Bank defines\textsuperscript{18} e-governance as the use of information and communication technologies by government agencies to transform relations with citizens, business and other arms of the government. It involves information technology enabled initiatives that are used for improving:

a. The interaction between government and citizens or government and business commonly known as e-services;

b. The internal government operations commonly known as e-administration; and

\begin{itemize}
\item \textbf{c.} External interaction among the members of society commonly known as e-society.
\end{itemize}

According to CSR Prabhu,\textsuperscript{19} e-governance is a form of e-business, which involves delivery of electronic services to the public. It also involves collaborating with business partners of the government by conducting electronic transactions with

\begin{table}
\begin{tabular}{|c|c|}
\hline
\textsuperscript{15} & Ibid., Section 15 \\
\textsuperscript{16} & Ibid., Section 16 \\
\textsuperscript{17} & Ibid., Proviso to Section 16 \\
\textsuperscript{18} & Vakul Sharma, \textit{Information Technology – Law and Practice}, 2010, p. 39 \\
\textsuperscript{19} & CSR Prabhu, \textit{E-governance Concepts and Case Studies}, 2004, p. 1 \\
\hline
\end{tabular}
\end{table}
them. It enables general public to interact with the government, through electronic means, for getting the desired services. In other words, e-governance means application of electronic means in the interactions between:

a. Government and Citizens (G2C)
b. Citizen and Government (C2G)
c. Government and Business (G2B)
d. Business and Government (B2G)
e. Internal government operation (G2G)

2. **Objectives of E-governance**

The main objective of e-governance is to simplify and improve governance and enable people’s participation in governance through mail and internet. E-governance is much more than just preparing some websites. It ranges from the use of internet for the dissemination of plain web based information at its simplest level to services and online transactions on the one hand and utilizing IT in the democratic process itself, i.e., election on the other.\(^{20}\)

E-governance is not only providing information about the various activities of the government to its citizens and other organizations but it involves citizens to communicate with government and participate in government decision-making.\(^{21}\) E-governance is applied in following ways:

a. Putting government laws and legislations online.
b. Putting information relating to government plans, budgets, expenditures and performances online.
c. Putting online key judicial decisions like environment decisions etc. which are important to citizens and create precedence for future actions.
d. Making available contact addresses of local, regional, national and international officials online.
e. Making available the reports of enquiry committees or commissions online.\(^{22}\)

---


\(^{21}\) Ritendra Goel, *Fundamentals of Information Technology*, 2009, p. 400

3. **Advantages of E-governance**

It has the following advantages:

a. Cheaper governance because it cuts financial and time costs.

b. Quicker governance, by producing the same output at the same total cost in less time.


d. More accountability of public servants for their actions and decisions.

e. Improves government efficiency and productivity.

f. Facilitates the delivery of government services to the citizens through procedural simplicity, speed and convenience.

g. Improves public image of the government by making government transparent.

4. **E-governance and Law in India**

Chapter 3 of the IT Act, 2000 (Sections 4-10A) deals with e-governance. Some important provisions are discussed as under:

i. **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 irrespective of anything contained in such law, such requirement shall be deemed to be satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference.\(^\text{23}\)

ii. **Legal recognition of electronic signatures**

   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 irrespective of anything contained in such law, such requirement shall be deemed to be 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.\(^\text{24}\)

---

\(^{23}\) Supra note 4, Section 4

\(^{24}\) *Ibid.*, Section 5
‘Signed’, to a person, mean affixing of his hand written signature or any mark on any document and the expression ‘signature’ shall be construed accordingly.\textsuperscript{25}

iii. Use of electronic records and electronic signatures in Government and its agencies

Where any law provides for:

\begin{itemize}
  \item The filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate government in a particular manner; or
  \item The use or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; or
  \item The receipt or payment of money in a particular manner,
\end{itemize}

then irrespective of anything contained in any other law for the time being in force, such requirement shall be deemed to be satisfied if such filing, issue, grant, receipt or payment is effected by means of such electronic form as may be prescribed by the appropriate government.\textsuperscript{26}

The appropriate government may, by rules, prescribe:

\begin{itemize}
  \item The manner and format in which such electronic records shall be filed, created or issued;
  \item The manner or method of payment of any fee or charges for filing, creation or issue any electronic record.\textsuperscript{27}
\end{itemize}

iv. Delivery of services by service provider

For the purposes of e-governance and for efficient delivery of services to the public through electronic means the appropriate government may, by notification in the Official Gazette, authorize any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify.\textsuperscript{28}

Service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor firm, or any other body or agency which

\textsuperscript{25} Ibid., Explanation to Section 5
\textsuperscript{26} Ibid., Section 6 (1)
\textsuperscript{27} Ibid., Section 6 (2)
\textsuperscript{28} Ibid., Section 6A (1)
has been granted permission by the appropriate government to offer services through electronic means in accordance with the policy governing such service sector.\textsuperscript{29}

The appropriate government may also authorize any service provider to collect, retain and appropriate such service charges, as may be prescribed by the appropriate government for the purpose of providing such services, from the person availing such service.\textsuperscript{30}

Further, the appropriate government may authorize the service provider to collect, retain and appropriate service charges even if there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.\textsuperscript{31}

The appropriate government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers.\textsuperscript{32}

However, the appropriate government may specify different scale of service charges for different types of services.\textsuperscript{33}

\section*{v. Retention of electronic records}

Where any law provides that documents, records or information shall be retained for any specified period, then that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form if:

- The information contained therein remains accessible so as to be usable for a subsequent reference;
- The electronic record is retained in the format in which it was originally generated, sent or received, or in the format which can be demonstrated to represent accurately the information originally generated, sent or received;
- The details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.\textsuperscript{34}

\begin{flushleft}
\textsuperscript{29} Ibid., Explanation to Section 6 A (1) \\
\textsuperscript{30} Ibid., Section 6A (2) \\
\textsuperscript{31} Ibid., Section 6A (3) \\
\textsuperscript{32} Ibid., Section 6A (4) \\
\textsuperscript{33} Ibid., Proviso to Section 6 A (4) \\
\textsuperscript{34} Ibid., Section 7 (1)
\end{flushleft}
However, the above provision will not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.\(^{35}\)

Further, the above said provision shall not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.\(^{36}\)

vi. **Audit of documents etc. maintained in electronic form**

Where any law for the time being in force contains provision for audit of documents, records or information, then such provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.\(^{37}\)

vii. **Publication of rule, regulation etc. in electronic gazette**

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette.\(^{38}\)

viii. **No right to insist government office etc. to interact in electronic form**

No right is conferred upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.\(^{39}\)

ix. **Power to make rules by Central Government in respect of electronic signature**

The Central Government may prescribe:

- The type of electronic signature;
- The manner and format in which electronic signature should be affixed;

---

\(^{35}\) *Ibid.*, Proviso to Section 7 (1)
\(^{36}\) *Ibid.*, Section 7 (2)
\(^{37}\) *Ibid.*, Section 7A
\(^{38}\) *Ibid.*, Section 8
\(^{39}\) *Ibid.*, Section 9
• The manner or procedure which facilitates identification of the person affixing the electronic signature;
• Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
• Any other matter which is necessary to give legal effect to electronic signatures.  

5. **E-governance Projects in India: An Overview**

In India, various governments are coming forward with a network of e-services and e-administration. However, most of them are rural centric rather than urban centric which are to be used by specific community residing in a municipal area, town, tehsil or district. In such e-governance projects, the user-friendly technology having local language is used for interaction. Further, most of these projects are financed by the local government. Following are some important e-governance projects:

i. **Gyandoot (Madhya Pradesh)**

Gyandoot is an intranet in Dhar district of Madhya Pradesh, connecting rural cyber cafes catering to the everyday needs of the masses. The website is an extension of Gyandoot intranet, for giving global access. This site offers following services:

• Commodity/Mandi Marketing Information System;
• Copies of Khasra, Khatauni and Maps;
• Online registration of applications;
• Income certificate
• Domicile certificate
• Caste certificate
• Holder’s passbook of land rights and loans.

ii. **Gramdoot (Rajasthan)**

This project was developed in Dabri Rampura (near Jaipur) and it provides various online facilities to the villagers, like Jamabandi (copies of land records), Shikayat online, Gramdak (rural e-mail account), Mandibhao (online rates), Gramhut

---

40 Ibid., Section 10
41 http://www.egovindia.org/egovportals.html accessed on 12.05.2010
42 http://www.gyandoot.net
(village bazaar), Vaivahiki (matrimonial service), Avedanpatra (application for driving licence), bank loans and ration cards and Praman Patra (issuance of domicile for caste, income certificate) etc.

iii. **Bhoomi (Karnataka)**

   This project involves computerization of more than 200 treasuries all over the State and it was mainly for computerization of land record system.

iv. **Warana (Maharashtra)**

   It was recently launched and the primary objective of this project is to demonstrate the effective use of IT infrastructure in the accelerated socio-economic development of 70 villages around Warana Nagar in the Kolhapur and Sangli districts. The existing cooperative structure has been used in concert with high speed VSATs to allow internet access to existing cooperative societies. The project aims to provide agricultural, medical and education information to villagers by establishing networked ‘facilitation booths’ in the villages.\(^{43}\)

v. **‘RajNidhi’ Information Kiosks (Rajasthan)**

   ‘RajNidhi’ is a web enabled information kiosk system developed jointly by Rajasthan State’s Department of Information Technology and Rajasthan State Agency for Computer Service (RajComp). On 23\(^{rd}\) March, 2000, Nayla became the first village of Rajasthan to have a ‘Raj Nidhi Information Kiosk’ when the US President, Mr. Bill Clinton visited this village to observe the functioning of Gram Panchayat.\(^{44}\)

vi. **Package for Effective Administration of Registration Laws Project – PEARL (Kerala)**

   The Government of Kerala has launched a project titled ‘PEARL’ for computerization of the Registration Department in the State.\(^{45}\)

vii. **Single Window Clearance System (Delhi)**

   The official website of the Delhi Government provides a ‘single window’ for all the citizen’s information needs and queries regarding the various public services of the Delhi Government, such as obtaining a driving licence or getting a marriage

---

\(^{43}\) [http://www.warna.com](http://www.warna.com)


\(^{45}\) [www.hindubusinessline.com/2000/08/12/stories/141260r1.htm](http://www.hindubusinessline.com/2000/08/12/stories/141260r1.htm)
registration certificate etc. Further, the site provides all relevant application forms for downloading and printing.\textsuperscript{46}

E. **ELECTRONIC CONTRACT**

As the name indicates e-contract means contract formed in electronic form. Further, e-contract is a part and parcel of e-commerce. Under the IT Act, 2000 earlier there was no provision relating to e-contract, but the IT (Amendment) Act, 2008 has inserted section 10A which confers the validity on contracts formed in e-form.

1. **Validity of contracts formed through electronic means**

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, are expressed in electronic form or by means of an electronic record, then such record shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.\textsuperscript{47}

2. **Attribution, Acknowledgement and Dispatch of Electronic Records**

i. **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;

c. By an information system programmed by or on behalf of the originator to operate automatically.\textsuperscript{48}

ii. **Acknowledgement of receipt**

a. **Acknowledgement not in a particular form or by a particular method**

Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic record must be given in particular form or by a particular method, then the acknowledgement may be given by any communication by the addressee, or any conduct of the addressee which is sufficient to indicate to the originator that the electronic record has been received.\textsuperscript{49}

\textsuperscript{46} http://www.delhigovt.nic.in

\textsuperscript{47} Supra note 4, Section 10A

\textsuperscript{48} Ibid., Section 11

\textsuperscript{49} Ibid., Section 12 (1)
b. **When electronic record is binding**

It is binding in the following 2 ways:

- **Where the originator has stipulated that the electronic record shall be binding only on receipt of acknowledgement**

  Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then unless acknowledgement has been so received by the originator, the electronic record shall be deemed to have been never sent by the originator.\(^{50}\)

- **Where the originator has not stipulated that the electronic record shall be binding only on receipt**

  Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or within a reasonable time if no time has been specified or agreed, then the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him, and where no acknowledgement is received within such time limit mentioned in the notice, then the electronic record shall be deemed to have been never sent by the originator.\(^{51}\)

iii. **Time and place of dispatch and receipt of electronic record**

a. **Time of dispatch of e-record**

  The dispatch of an e-record occurs when it enters a computer resource outside the control of the originator.\(^{52}\)

b. **Time of receipt of e-record**

  The time of receipt of an e-record shall be determined in the following manner:

  i. Where the addressee has assigned a computer resource for the purpose of receiving e-records and the e-record is received in a designed computer resource then receipt occurs at the time when e-record enters the designated computer resource; or a computer resource of the addressee that is not the

\(^{50}\) *Ibid.*, Section 12 (2)

\(^{51}\) *Ibid.*, Section 12 (3)

\(^{52}\) *Ibid.*, Section 13 (1)
designated computer resource then receipt occurs at a time when the e-record is retrieved by the addressee.

ii. Where the addressee has not designated a computer resource nor specified any timings for receipt of e-record then the receipt occurs when e-record enters the computer resource of the addressee. 53

c. **Place of dispatch of e-record**

An e-record is deemed to be dispatched at the place where the originator has his place of business. 54

d. **Place of receipt of e-record**

An e-record is deemed to be received at the place where the addressee has his place of business. 55

F. **REGULATION OF CERTIFYING AUTHORITIES**

The regulation of Certifying Authority (CA) is a statutory function of the Controller of Certifying Authority (CCA) and under the IT Act he has to act as administrative authority rather than quasi-judicial body.

1. **Appointment of Controller and other Officers**

The central government may, by notification in the official gazette, appoint a Controller of Certifying Authorities (CCA) for the purposes of IT Act and may also appoint such number of deputy controllers and assistant controllers, other officers and employees as it deems fit. 56

i. **Functions to be performed by the CCAs**

The Controller shall discharge his function subject to the general control and directions of the central government. 57

ii. **Function to be performed by Deputy CCAs or Assistant CCAs**

The deputy and assistant controllers shall perform the functions assigned to them by the controller under the general superintendence and control of the controller. 58

---

53 *Ibid.*, Section 13 (2)
54 *Ibid.*, Section 13 (3)
56 *Ibid.*, Section 17 (1)
57 *Ibid.*, Section 17 (2)
58 *Ibid.*, Section 17 (3)
iii. **Qualification, experience, terms and conditions of service**

The qualifications, experience and terms and conditions of service of controller, deputy controllers, assistant controllers, other officers and employees shall be such as may be prescribed by the central government. 59

iv. **Head office and branch office of the Controller**

The head office and branch office of the controller shall be at such places as the central government may specify. 60

2. **Functions of Controller**

The controller may perform all or any of the following functions:

(i) Exercising supervision over the activities of the certifying authorities;

(ii) Certifying public keys of the certifying authorities;

(iii) Laying down the standards to be maintained by the certifying authorities;

(iv) Specifying the qualification and experience which employees of the certifying authorities should possess;

(v) Specifying the form and content of an electronic signature certificate and the key;

(vi) Laying down the duties of certifying authorities. 61

3. **Recognition of Foreign Certifying Authorities**

With the previous approval of the central government the controller may recognize any foreign certifying authority as a certifying authority for the purposes of this Act. 62

(i) **Electronic signature certificate issued by Foreign Certifying Authorities**

The electronic signature certificate issued by such authority shall be valid. 63

(ii) **Revocation of licence of foreign certifying authority**

Where the controller is satisfied that any foreign certifying authority has contravened any of the conditions subject to which it was granted recognition then he may revoke such recognition after recording the reasons for it in writing. 64

---

59 *Ibid.*, Section 17 (4)
60 *Ibid.*, Section 17 (5)
61 *Ibid.*, Section 18
62 *Ibid.*, Section 19 (1)
63 *Ibid.*, Section 19 (2)
64 *Ibid.*, Section 19 (3)
4. **Licence to issue electronic signature certificates**

Any person may make an application to the controller for a licence to issue electronic signature certificates. 65

i. **Requirement for granting licence**

No licence shall be issued unless the applicant fulfils 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. 66

ii. **Validity period of licence**

A licence shall be valid for such period as may be prescribed by the central government. It shall not be transferable or heritable. 67

5. **Application for licence**

Every application for issue of a licence shall be in such form as may be prescribed by the central government. 68

Every application 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 Rs. 25,000, as may be prescribed by the central government;

d. Such other documents as may be prescribed by the central government. 69

6. **Renewal of licence**

An application for renewal of licence shall be in such form and accompanied by such fee, not exceeding Rs. 25,000, as may be prescribed by the central government. It shall be made not less than 45 days before the date of expiry of the period of validity of the licence. 70

---

65 Ibid., Section 21 (1)
66 Ibid., Section 21 (2)
67 Ibid., Section 21 (3)
68 Ibid., Section 22 (1)
69 Ibid., Section 22 (2)
70 Ibid., Section 23
7. **Procedure for grant or rejection of licence**

On receipt of application and after considering the documents accompanying the application and other factors, the controller may grant the licence or reject the application\(^{71}\). However, before rejecting the application, the applicant should be given an opportunity of being heard.\(^{72}\)

G. **ELECTRONIC SIGNATURE CERTIFICATE**

1. **Application for Granting of Electronic Signature Certificate**

   Any person may make an application to the Certifying Authority for the issue of an Electronic Signature Certificate in such form as may be prescribed by the Central Government.\(^{73}\)

2. **Fee**

   Every such application shall be accompanied by such fee not exceeding Rs. 25,000 as may be prescribed by the Central Government.\(^{74}\)

   Different fees may be prescribed for different classes of applicants.\(^{75}\)

3. **Documents to be attached with the application**

   Every such application must be accompanied by a certification practice statement and where no such statement is given then a statement containing particulars as may be specified by regulations.\(^{76}\)

   The ‘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.\(^{77}\)

4. **Granting of Electronic Signature Certificate**

   The Certifying Authority, after considering the application and certification practice statement or any other statement and after making such inquiries as it thinks fit, shall grant electronic signature certificate. However, where it is not satisfied, it may reject the application but it must record the reasons in writing for doing so.\(^{78}\)

---

\(^{71}\) *Ibid.*, Section 24

\(^{72}\) *Ibid.*, Proviso to Section 24

\(^{73}\) *Ibid.*, Section 35 (1)

\(^{74}\) *Ibid.*, Section 35 (2)

\(^{75}\) *Ibid.*, Proviso to Section 35 (2)

\(^{76}\) *Ibid.*, Section 35 (3)

\(^{77}\) *Ibid.*, Section 2 (1) (h)

\(^{78}\) *Ibid.*, Section 35 (4)
No application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.  

5. **Representation upon issuance of Digital Signature Certificate**

While issuing a Digital Signature Certificate, the Certifying Authority shall certify that:

a. It has complied with the provisions of IT Act, 2000, and the rules and regulations made thereunder;  

b. It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;  

c. The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;  

d. The subscriber holds a private key which is capable of creating a digital signature;  

e. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;  

f. The subscriber’s public key and private key constitute a functioning key pair;  

g. The information contained in the Digital Signature Certificate is accurate;  

and  

h. It has no knowledge of any material fact, which if had been included in the Digital Signature Certificate would adversely affect the reliability of the above mentioned representations.  

6. **Suspension of Digital Signature Certificate**

The Certifying Authority which has issued a Digital Signature Certificate may suspend it:

---

78 *Ibid.*, Proviso to Section 35 (4)  
79 *Ibid.*, Section 36 (a)  
80 *Ibid.*, Section 36 (b)  
81 *Ibid.*, Section 36 (c)  
82 *Ibid.*, Section 36 (ca)  
83 *Ibid.*, Section 36 (cb)  
84 *Ibid.*, Section 36 (d)  
85 *Ibid.*, Section 36 (e)  
86 *Ibid.*, Section 36 (f)  
87 *Ibid.*, Section 36 (f)
On receipt of request to that effect either by the subscriber mentioned in the Digital Signature Certificate or any other authorized person;

Where in the opinion of the Certifying Authority, the Digital Signature Certificate must be suspended in public interest.\(^{88}\)

The Digital Signature Certificate can be suspended for a maximum of 15 days. Further, a reasonable opportunity if being heard should be given to the subscriber to continue suspension after 15 days.\(^{89}\)

After suspension, the Certifying Authority must communicate the same to the subscriber.\(^{90}\)

**7. Revocation of Digital Signature Certificate**

The Certifying Authority may revoke a Digital Signature Certificate issued by it in the following cases:

i. Where a request to that effect is made by the subscriber or any other person authorized by him; or

ii. upon the death of the subscriber; or

iii. upon the dissolution of the firm or winding up of the company, where the subscriber is a company or firm.\(^{91}\)

iv. where in the opinion of the Certifying Authority:

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

b. A requirement for the issuance of Digital Signature Certificate was not satisfied;

c. The Certifying Authority’s private key or security system was compromised in a manner which materially affects the Digital Signature Certificate’s reliability;

d. The subscriber has been declared insolvent or dead, or where the subscriber is a firm or company, it has been dissolved or wound up or otherwise ceased to exist\(^{92}\)

---

\(^{88}\) Ibid., Section 37 (1)

\(^{89}\) Ibid., Section 37 (2)

\(^{90}\) Ibid., Section 37 (3)

\(^{91}\) Ibid., Section 38 (1)

\(^{92}\) Ibid., Section 38 (2)
Further, a Digital Signature Certificate shall not be revoked without giving a reasonable opportunity of being heard to the subscriber.\textsuperscript{93} However, on revocation, the Certifying Authority shall communicate the matter to the subscriber.\textsuperscript{94}

8. **Notice of suspension or revocation**

Where Digital Signature Certificate has been suspended or revoked, the Certifying Authority shall publish a notice of such suspension or revocation in the repository specified in the Digital Signature Certificate for publication of such notice.\textsuperscript{95} However, where one or more repositories are specified, then the Certifying Authority shall publish notices of such suspension or revocation in all such repositories.\textsuperscript{96}

H. **SUBSCRIBER**

1. **Definition of Subscriber**

Subscriber means a person in whose name the Electronic Signature Certificate is issued.\textsuperscript{97}

2. **Procedure for becoming a subscriber**

Following procedure is followed for becoming a subscriber under the Information Technology Act, 2000

a. Apply to the Local Registration Authority of a licensed Certifying Authority in a prescribed application form for granting Digital Signature Certificate or Electronic Signature Certificate.

b. Select the particular class of certificate in which the applicant is interested.

c. Enter into an agreement with the Local Registration Authority.

d. Generate key pair in a secure medium and prove the possession of private key corresponding to public key.

e. The Local Registration Authority shall forward the application to licensed Certifying Authority, if he is satisfied, after verifying the relevant documents that the applicant is genuine and the application is in accordance with the provisions of law. Now the licensed Certifying Authority shall generate

\textsuperscript{93} Ibid., Section 38 (3)
\textsuperscript{94} Ibid., Section 38 (4)
\textsuperscript{95} Ibid., Section 39 (1)
\textsuperscript{96} Ibid., Section 39 (2)
\textsuperscript{97} Ibid., Section 2 (1) (zg)
Digital Signature Certificate. Subscriber shall download the Digital Signature Certificate from licensed Certifying Authority’s website.

f. The subscriber shall verify the contents of Digital Signature Certificate and shall accept it.

g. The Certifying Authority shall publish such Digital Signature Certificate.

3. **Duties of Subscriber**

   Following are the important duties of the subscriber under the IT Act, 2000:

   i. **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.\(^98\)

   ii. **Duties of subscriber of Electronic Signature Certificate**

   In respect of Electronic Signature Certificate, the subscriber shall perform such duties as may be prescribed.\(^99\)

   iii. **Acceptance of Digital Signature Certificate**

   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

   c. Otherwise demonstrates his approval of the Digital Signature Certificate in any manner.\(^100\)

   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;

---

\(^{98}\) *Ibid.*, Section 40

\(^{99}\) *Ibid.*, Section 40A

\(^{100}\) *Ibid.*, Section 41 (1)
c. All information in the Digital Signature Certificate, which is within the knowledge of the subscriber, is true.\(^{101}\)

iv. **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.\(^{102}\)

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.\(^{103}\)

The subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.\(^{104}\)

I. **PENALTIES, COMPENSATION AND ADJUDICATION**

1. **Penalty and compensation for damage to computer, computer system, etc.**

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network does any of the following acts then he shall be liable to pay damages by way of compensation to the person so affected –

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 database or any other programmes residing in such computer, computer system or computer network;

\(^{101}\) *Ibid.*, Section 41 (2)

\(^{102}\) *Ibid.*, Section 42 (1)

\(^{103}\) *Ibid.*, Section 42 (2)

\(^{104}\) *Ibid.*, Explanation to Section 42 (2)
e. Disrupts or causes disruption of any computer, computer system or computer network;

f. Denies or causes the denial of access to any person authorized 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. 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.\textsuperscript{105}

‘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.\textsuperscript{106}

‘Computer database’ means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in the formalized 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.\textsuperscript{107}

‘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

\textsuperscript{105} Ibid., Section 43
\textsuperscript{106} Ibid., Explanation (i) to Section 43
\textsuperscript{107} Ibid., Explanation (ii) to Section 43
a programme, data or instruction is executed or some other event takes place in that 
computer resource.108

‘Damage’ means to destroy, alter, delete, add, modify or rearrange any 
computer resource by any means.109

‘Computer source code’ means the listing of programmes, computer 
commands, design and layout and programme analysis of computer resource in any 
form.110

2. **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.111

‘Body corporate’ means any company and includes a firm, sole proprietorship 
or other association of individuals engaged in commercial or professional activities.112

‘Reasonable security practices and procedures’ means security practices and 
procedures designed to protect such information from unauthorized 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.113

‘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.114

---

108 *Ibid.*, Explanation (iii) to Section 43
109 *Ibid.*, Explanation (iv) to Section 43
110 *Ibid.*, Explanation (v) to Section 43
111 *Ibid.*, Section 43 A; See also Ranjan Mukherjee, “Data Privacy – The Scenario Prevailing in India”, 
*Chartered Secretary*, November 2007, p. 1509
112 *Ibid.*, Explanation (i) to Section 43A
113 *Ibid.*, Explanation (ii) to Section 43A
114 *Ibid.*, Explanation (iii) to Section 43A
3. **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, then he shall be liable to a penalty not exceeding Rs. 1.5 lakhs 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, then he shall be liable to a penalty not exceeding Rs. 5,000 for every day during which such failure continues;
   
   c. Maintain books of account or records, fails to maintain the same, then he shall be liable to a penalty not exceeding Rs. 10,000 for every day during which the failure continues.115

4. **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 compensation not exceeding Rs. 25,000 to the person affected by such contravention or a penalty not exceeding Rs. 25, 000.116

5. **Power to adjudicate**

   In order to decide 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, then the Central Government shall 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.117

---

115 *Ibid.*, Section 44
116 *Ibid.*, Section 45
117 *Ibid.*, Section 46 (1)
The adjudicating officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed Rs. 5 crore.\textsuperscript{118}

However, where the claim for injury or damage exceeds Rs. 5 crore then the jurisdiction would vest with the competent court.\textsuperscript{119}

The adjudicating officer shall give the accused a reasonable opportunity for making representation in the matter. If, after inquiry, he is satisfied that the person has committed the contravention then he may impose such penalty or award such compensation as he thinks fit.\textsuperscript{120}

The person to be appointed as adjudicating officer shall possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.\textsuperscript{121}

Where more than one adjudicating officers are appointed, then the Central Government shall specify the matters and places with respect to which such officers shall exercise their jurisdiction.\textsuperscript{122}

Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal u/s 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, 1860;

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.\textsuperscript{123}

6. \textbf{Factors to be taken into account by the adjudicating officer}

While adjudging the quantum of compensation, the adjudicating officer shall have due regard to the following factors, namely –

a. The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

b. The amount of loss caused to any person as a result of the default;

\textsuperscript{118} \textit{Ibid.}, Section 46 (1A)

\textsuperscript{119} \textit{Ibid.}, Proviso to Section 46 (1A)

\textsuperscript{120} \textit{Ibid.}, Section 46 (2)

\textsuperscript{121} \textit{Ibid.}, Section 46 (3)

\textsuperscript{122} \textit{Ibid.}, Section 46 (4)

\textsuperscript{123} \textit{Ibid.}, Section 46 (5)
c. The repetitive nature of the default.  

J. CYBER APPELLATE TRIBUNAL

1. Establishment of Cyber Appellate Tribunal

The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.\(^{125}\)

The Central Government shall also specify in the notification, the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.\(^{126}\)

2. Composition of Cyber Appellate Tribunal

The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other members, as the Central Government may, by notification in the Official Gazette, appoint.\(^{127}\)

The selection of Chairperson and members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.\(^{128}\)

The jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof.\(^{129}\) A Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.\(^{130}\) The Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, specify by notification in the Official Gazette.\(^{131}\) By notification in the Official Gazette, the Central Government shall specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.\(^{132}\)

The Chairperson of the Cyber Appellate Tribunal may transfer a member of such Tribunal from one Bench to another Bench.\(^{133}\)

\(^{124}\) Ibid., Section 47
\(^{125}\) Ibid., Section 48 (1)
\(^{126}\) Ibid., Section 48 (2)
\(^{127}\) Ibid., Section 49 (1)
\(^{128}\) Ibid., Section 49 (2)
\(^{129}\) Ibid., Section 49 (3) (a)
\(^{130}\) Ibid., Section 49 (3) (b)
\(^{131}\) Ibid., Section 49 (3) (c)
\(^{132}\) Ibid., Section 49 (3) (d)
\(^{133}\) Ibid., Section 49 (4)
If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, then the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.\textsuperscript{134}

3. \textbf{Qualification for appointment as Chairperson and Members of Cyber Appellate Tribunal}

A person can be appointed as a Chairperson of the Cyber Appellate Tribunal if he is, or has been, or is qualified to be, a Judge of a High Court.\textsuperscript{135}

The Members of the Cyber Appellate Tribunal, except the Judicial Member, shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs.\textsuperscript{136}

A person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than 1 year, or Joint Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than 7 years.\textsuperscript{137}

The Judicial Member of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than 1 year or Grade I post of that service for a period of not less than 5 years.\textsuperscript{138}

4. \textbf{Term of office, conditions of service, etc., of Chairperson and Members}

The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of 5 years from the date on which he enters upon his office or until he attains the age of 65 years, whichever is earlier.\textsuperscript{139}

\begin{itemize}
\item \textsuperscript{134} \textit{Ibid.}, Section 49 (5)
\item \textsuperscript{135} \textit{Ibid.}, Section 50 (1)
\item \textsuperscript{136} \textit{Ibid.}, Section 50 (2)
\item \textsuperscript{137} \textit{Ibid.}, Proviso to Section 50 (2)
\item \textsuperscript{138} \textit{Ibid.}, Section 50 (3)
\item \textsuperscript{139} \textit{Ibid.}, Section 51 (1)
\end{itemize}
Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.\(^{140}\)

An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, shall have to retire from service before joining as such Chairperson or Member.\(^{141}\)

5. **Salary, allowances and other terms and conditions of service of Chairperson and Members**

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of the Cyber Appellate Tribunal shall be such as may be prescribed.\(^{142}\)

6. **Power of superintendence, direction, etc.**

The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.\(^{143}\)

7. **Distribution of business among Benches**

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.\(^{144}\)

8. **Power of Chairperson to transfer cases**

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or *suo motu* without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench for disposal to any other Bench.\(^{145}\)

\(^{140}\) *Ibid.*, Section 51 (2)

\(^{141}\) *Ibid.*, Section 51 (3)

\(^{142}\) *Ibid.*, Section 52

\(^{143}\) *Ibid.*, Section 52A

\(^{144}\) *Ibid.*, Section 52 B

\(^{145}\) *Ibid.*, Section 52 C
9. **Decision by majority**

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.\(^{146}\)

10. **Filling up of vacancies**

If, for reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or Member of a Cyber Appellate Tribunal, then the Central Government shall appoint another person to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.\(^{147}\)

11. **Resignation and removal**

The Chairperson or Member of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office.\(^{148}\)

However, the said presiding officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of 3 months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.\(^{149}\)

The presiding officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehavior or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.\(^{150}\)

---

\(^{146}\) *Ibid.*, Section 52 D

\(^{147}\) *Ibid.*, Section 53

\(^{148}\) *Ibid.*, Section 54 (1)

\(^{149}\) *Ibid.*, Proviso to Section 54 (1)

\(^{150}\) *Ibid.*, Section 54 (2)
The Central Government may, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid Presiding Officer.\textsuperscript{151}

**12. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings**

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.\textsuperscript{152}

**13. Staff of the Cyber Appellate Tribunal**

The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.\textsuperscript{153}

The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Chairperson.\textsuperscript{154}

The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.\textsuperscript{155}

**14. Appeal to Cyber Appellate Tribunal**

Any person aggrieved by an order made by the controller or an adjudicating officer under the IT act, 2000 may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.\textsuperscript{156}

\begin{itemize}
  \item **i. No appeal against order made with the consent of parties**
  
  No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.\textsuperscript{157}
  \item **ii. Limitation period for filing an appeal**
  
  Every appeal shall be filed within a period of 45 days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the
\end{itemize}

\textsuperscript{151} Ibid., Section 54 (3)
\textsuperscript{152} Ibid., Section 55
\textsuperscript{153} Ibid., Section 56 (1)
\textsuperscript{154} Ibid., Section 56 (2)
\textsuperscript{155} Ibid., Section 56 (3)
\textsuperscript{156} Ibid., Section 57 (1)
\textsuperscript{157} Ibid., Section 57 (2)
person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed.\textsuperscript{158}

However, the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was sufficient cause for not filing it within that period.\textsuperscript{159}

iii. **Order of the Cyber Appellate Tribunal**

On receipt of an appeal, the Cyber Appellate Tribunal may, after giving the parties to appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.\textsuperscript{160}

iv. **Copy of the order**

The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.\textsuperscript{161}

v. **Limitation period for deciding an appeal**

The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within 6 months from the date of receipt of the appeal.\textsuperscript{162}

15. **Procedure and powers of the Cyber Appellate Tribunal**

i. **Procedure of the Cyber Appellate Tribunal**

The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of the IT Act, 2000 and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.\textsuperscript{163}

ii. **Powers of the Cyber Appellate Tribunal**

For the purposes of discharging its functions under the IT Act, 2000, the Cyber Appellate Tribunal shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:

\begin{itemize}
  \item \textsuperscript{158} *Ibid.*, Section 57 (3)
  \item \textsuperscript{159} *Ibid.*, Proviso to Section 57 (3)
  \item \textsuperscript{160} *Ibid.*, Section 57 (4)
  \item \textsuperscript{161} *Ibid.*, Section 57 (5)
  \item \textsuperscript{162} *Ibid.*, Section 57 (6)
  \item \textsuperscript{163} *Ibid.*, Section 58 (1)
\end{itemize}
a. Summoning and enforcing the attendance of any person and examining him on oath;
b. Requiring the discovery and production of documents or other electronic records;
c. Receiving evidence on affidavits;
d. Issuing commissions for the examination of witnesses or documents;
e. Reviewing its decisions;
f. Dismissing an application for default or deciding it *ex parte*;
g. Any other matter which may be prescribed.\textsuperscript{164}

**iii. Proceedings of the Cyber Appellate Tribunal**

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228 and for the purposes of Section 196 of the Indian Penal Code, 1860, and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.\textsuperscript{165}

**16. Right to legal representation**

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.\textsuperscript{166}

**17. Limitation Period**

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.\textsuperscript{167}

**18. Civil court not to have jurisdiction**

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by this Act.\textsuperscript{168}

\textsuperscript{164} *Ibid.*, Section 58 (2)
\textsuperscript{165} *Ibid.*, Section 58 (3)
\textsuperscript{166} *Ibid.*, Section 59
\textsuperscript{167} *Ibid.*, Section 60
\textsuperscript{168} *Ibid.*, Section 61
19. **Appeal to high court**

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order.\(^{169}\)

However, if the High Court is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, then it may allow the appeal to be filed within a further period not exceeding 60 days.\(^{170}\)

20. **Compounding of contraventions**

Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the controller or such other officer or the adjudicating officer may specify.\(^{171}\)

However such sum shall not exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.\(^{172}\)

Further, it shall not apply to a person who commits the same or similar contravention within a period of 3 years from the date on which the first contravention, committed by him, was compounded.\(^{173}\)

Any second or subsequent contravention committed after the expiry of a period of 3 years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.\(^{174}\)

Where any contravention has been compounded, no proceeding or further proceeding shall be taken against the person guilty of such contravention, in respect of the contravention so compounded.\(^{175}\)

---

\(^{169}\) *Ibid.*, Section 62

\(^{170}\) *Ibid.*, Proviso to Section 62

\(^{171}\) *Ibid.*, Section 63 (1)

\(^{172}\) *Ibid.*, Proviso to Section 63 (1)

\(^{173}\) *Ibid.*, Section 63 (2)

\(^{174}\) *Ibid.*, Explanation to Section 63 (2)

\(^{175}\) *Ibid.*, Section 63 (3)
21. **Recovery of penalty and compensation**

A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate shall be suspended till the penalty is paid.¹⁷⁶

K. **OFFENCES**

1. **Tampering with computer source documents**

Any person who knowingly or intentionally conceals, destroys or alters, or causes another to conceal, destroy or alter any computer source code used for a computer, computer program, 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 3 years or with fine which may extend up to Rs. 2 lakh or with both.¹⁷⁷

The ‘computer source code’ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.¹⁷⁸

2. **Computer related offences**

Any person who, dishonestly or fraudulently, does any act referred to in Section 43, shall be punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to Rs. 5 lakh or with both.¹⁷⁹

The words ‘dishonestly’ and ‘fraudulently’ shall have the same meaning assigned to them in the Indian Penal Code.¹⁸²

3. **Punishment for sending offensive messages through communication service, etc.**

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

a. Any information that is grossly offensive or has a menacing character; or

---

¹⁷⁶ *Ibid.*, Section 64
¹⁷⁷ *Ibid.*, Section 65
¹⁷⁸ *Ibid.*, Explanation to Section 65
¹⁷⁹ *Ibid.*, Section 66
¹⁸⁰ The Indian Penal Code, 1860; Section 24
¹⁸¹ *Ibid.*, Section 25
¹⁸² *Supra note* 178
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; or
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 3 years and with fine.¹³³

The ‘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.¹³⁴

4. Punishment for dishonestly receiving stolen computer resource or communication device

Any person who, dishonestly received 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 3 years or with fine which may extend to Rs. 1 lakh or with both.¹³⁵

5. Punishment for identity theft

Any person who, fraudulently or dishonestly makes 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 3 years and shall also be liable to fine which may extend to Rs. 1 lakh.¹³⁶

6. Punishment for cheating by personation by using computer resource

Any person who, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either

---
¹³³ The Information Technology Act, 2000; Section 66A
¹³⁴ Ibid., Section 2 (1) (ha)
¹³⁵ Ibid., Section 66B
¹³⁶ Ibid., Section 66 C
description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1 lakh.187

7. **Punishment for violation of privacy**

Any person who, 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 3 years or with fine not exceeding Rs. 2 lakh, or with both.188

‘Transmit’ means to electronically send a visual image with the intent that it be viewed by a person or persons.189

‘Capture’ with respect to an image, means to videotape, photograph, film or record by any means.190

‘Private area’ means the naked or undergarment clad genitals, pubic area, buttocks or female breast.191

‘Publishes’ means reproduction in the printed or electronic form and making it available for public.192

8. **Punishment for Cyber Terrorism**

A person commits the offence of cyber terrorism if he,

(i). 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 –

a. denies or causes the denial of access to any person authorized to access computer resource; or

b. attempts to penetrate or access a computer resource without authorization or by exceeding authorized access; or

c. introduces or causes 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 knowing that it is likely to cause damage

187 *Ibid.*, Section 66 D
188 *Ibid.*, Section 66 E
189 *Ibid.*, Explanation (a) to Section 66E
190 *Ibid.*, Explanation (b) to Section 66E
191 *Ibid.*, Explanation (c) to Section 66E
192 *Ibid.*, Explanation (d) to Section 66E
or destruction of supplies or services essential to the life of the community, or adversely affect the critical information infrastructure specified u/s 70 (ii). Knowingly or intentionally accesses or penetrates a computer resource without authorization or exceeding authorized 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.\textsuperscript{193}

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.\textsuperscript{194}

9. **Punishment for publishing or transmitting obscene material in electronic form**

Any person who, publishes or transmits or causes to be published or transmitted 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 3 years and with fine which may extend to Rs. 5 lakh and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to 5 years and also with fine which may extend to Rs. 10 lakh.\textsuperscript{195}

10. **Punishment for publishing or transmitting of material containing sexually explicit act etc. in electronic form**

Any person who, 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

\textsuperscript{193} Ibid., Section 66 F (1)
\textsuperscript{194} Ibid., Section 66 F (2)
\textsuperscript{195} Ibid., Section 67
for a term which may extend to 5 years and with fine which may extend to Rs. 10 lakh, and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to Rs. 10 lakh.\textsuperscript{196}

11. **Punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form**

Any person who,

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 5 years and with fine which may extend to Rs. 10 lakh and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to Rs. 10 lakh.\textsuperscript{197}

However, these provisions does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –

a. 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

\textsuperscript{196} Ibid., Section 67 A
\textsuperscript{197} Ibid., Section 67 B
b. which is kept or used for *bona fide* heritage or religious purposes.\(^{198}\)

12. **Preservation and retention of information by intermediaries**

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.\(^{199}\)

Any intermediary who intentionally or knowingly contravenes the above duty shall be punished with imprisonment for a term which may extend to 3 years and also be liable to fine.

13. **Power of Controller to give directions**

The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on of such activities as specified in the order if those are necessary to ensure compliance with the provisions of IT Act, 2000, rules or any regulations made thereunder.\(^{200}\)

Any person, who intentionally or knowingly fails to comply with any abovementioned order, shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding 2 years or a fine not exceeding Rs. 1 lakh or both.\(^{201}\)

14. **Power to issue directions for interception or monitoring or decryption of any information through any computer resource**

Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, is satisfied that it is necessary or expedient to do so 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, then it may by an 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.\(^{202}\)

---

\(^{198}\) *Ibid.*, Proviso to Section 67B
\(^{199}\) *Ibid.*, Section 67 C (1)
\(^{200}\) *Ibid.*, Section 68 (1)
\(^{201}\) *Ibid.*, Section 68 (2)
\(^{202}\) *Ibid.*, Section 69 (1)
The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.203

The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency, 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, monitor or decrypt the information; or

c. Provide information stored in the computer resource.204

The subscriber or intermediary or any person who fails to assist such agency shall be punished with imprisonment for a term which may extend to 7 years and shall also be liable to fine.205

15. **Power to issue directions for blocking for public access of any information through any computer resource**

Where the Central Government or any of its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient to do so, in the interest of 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, then it may, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.206

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.207

The intermediary who fails to comply with such direction shall be punished with imprisonment for a term which may extend to 7 years and shall also be liable to fine.208

---

203 Ibid., Section 69 (2)
204 Ibid., Section 69 (3)
205 Ibid., Section 69 (4)
206 Ibid., Section 69 A (1)
207 Ibid., Section 69 A (2)
208 Ibid., Section 69 A (3)
16. **Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security**

To enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, the Central Government may 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.\(^\text{209}\)

The intermediary or any person-in-charge of the computer resource, when called upon by such agency, shall 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.\(^\text{210}\)

The procedure and safeguard for monitoring and collecting traffic data or information, shall be such as may be prescribed.\(^\text{211}\)

Any intermediary who intentionally or knowingly contravenes the above said duty shall be punished with imprisonment for a term which may extend to 3 years and shall also be liable to fine.\(^\text{212}\)

17. **Protected system**

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.\(^\text{213}\)

‘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.\(^\text{214}\)

The appropriate Government may, by order in writing, authorize the persons to access such protected systems.\(^\text{215}\)

\(^{209}\) *Ibid.*, Section 69 B (1)

\(^{210}\) *Ibid.*, Section 69 B (2)

\(^{211}\) *Ibid.*, Section 69 B (3)

\(^{212}\) *Ibid.*, Section 69 B (4)

\(^{213}\) *Ibid.*, Section 70 (1)

\(^{214}\) *Ibid.*, Explanation to Section 70 (1)

\(^{215}\) *Ibid.*, Section 70 (2)
Any person who secures access or attempts to secure access to a protected system in contravention of the above provisions shall be punished with imprisonment of either description for a term which may extend to 10 years and shall also be liable to fine.\textsuperscript{216}

The Central Government shall prescribe the information security practices and procedures for such protected system.\textsuperscript{217}

18. **National nodal agency**

The Central Government may, by notification in the Official Gazette, designate any organization of the Government as the national nodal agency in respect of the Critical Information Infrastructure Protection.\textsuperscript{218}

Such designated national nodal agency shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.\textsuperscript{219}

Further, such agency shall perform its functions and duties in the prescribed manner.\textsuperscript{220}

19. **Indian Computer Emergency Response Team to serve as national agency for incident response**

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.\textsuperscript{221}

The Central Government shall provide such agency with a Director-General and such other officers and employees as may be prescribed.\textsuperscript{222}

The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.\textsuperscript{223}

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;

\textsuperscript{216} Ibid., Section 70 (3)
\textsuperscript{217} Ibid., Section 70 (4)
\textsuperscript{218} Ibid., Section 70 A (1)
\textsuperscript{219} Ibid., Section 70 A (2)
\textsuperscript{220} Ibid., Section 70 A (3)
\textsuperscript{221} Ibid., Section 70 B (1)
\textsuperscript{222} Ibid., Section 70 B (2)
\textsuperscript{223} Ibid., Section 70 B (3)
b. Forecast and alerts of cyber security incidents;
c. Emergency measures for handling cyber security incidents;
d. Coordination of cyber incidents response activities;
e. Issuing guidelines, advisories, vulnerability notes and whitepapers 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.  

The manner of performing functions and duties of the agency shall be such as may be prescribed.

For performing its functions, the agency may call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person.

Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction shall be punishable with imprisonment for a term which may extend to 1 year or with fine which may extend to Rs. 1 lakh or with both.

However, no court shall take cognizance of any offence except on a complaint made by an officer authorized in this behalf by the agency.

20. **Penalty for misrepresentation**

Any person who makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or Electronic Signature Certificate shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

21. **Penalty for breach of confidentiality and privacy**

If any person who, in pursuance 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 and 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 2 years or with fine which may extend to Rs. 1 lakh or with both.230

22. **Punishment for disclosure of information in breach of lawful contract**

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 3 years or with fine which may extend to Rs. 5 lakh or with both.231

23. **Penalty for publishing Electronic Signature Certificate false in certain particulars**

No person shall publish an 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 electronic signature created prior to such suspension or revocation.232

Any person who contravenes above provisions shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.233

---

230 Ibid., Section 72
231 Ibid., Section 72 A
232 Ibid., Section 73 (1)
233 Ibid., Section 73 (2)
24. **Publication for fraudulent purpose**

Any person, who knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.\(^{234}\)

25. **Act to apply for offence or contravention committed outside India**

The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.\(^{235}\)

However, for such liability the act or conduct constituting the offence or contravention should involve a computer, computer system or computer network located in India.\(^ {236}\)

26. **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 thereunder has been or is being contravened, shall be liable to confiscation.\(^ {237}\)

However, 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 thereunder, then 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 authorized by this Act against the person contravening the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.\(^ {238}\)

---

\(^{234}\) *Ibid.*, Section 74

\(^{235}\) *Ibid.*, Section 75 (1)

\(^{236}\) *Ibid.*, Section 75 (2)

\(^{237}\) *Ibid.*, Section 76 (1)

\(^{238}\) *Ibid.*, Section 76 (2)
27. **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.\(^{239}\)

28. **Compounding of offences**

A court of competent jurisdiction may compound offences, except the offences for which the punishment for life or imprisonment for a term exceeding 3 years has been provided, under this Act.\(^{240}\) However, 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 different kind.\(^{241}\)

Further, 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.\(^{242}\)

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 Sections 265 B and 265 C of the Code of Criminal Procedure, 1973 shall apply.\(^{243}\)

29. **Offences with 3 years imprisonment to be bailable**

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of 3 years and above shall be cognizable and the offence punishable with imprisonment of 3 years shall be bailable.\(^{244}\)

30. **Power to investigate offences**

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.\(^{245}\)

\(^{239}\) *Ibid.*, Section 77
\(^{240}\) *Ibid.*, Section 77 A (1)
\(^{241}\) *Ibid.*, Proviso to Section 77 A (1)
\(^{242}\) *Ibid.*
\(^{243}\) *Ibid.*, Section 77 A (2)
\(^{244}\) *Ibid.*, Section 77 B
Table: Offences under the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Section</th>
<th>Offence</th>
<th>Punishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>65</td>
<td>Tampering with computer source documents</td>
<td>Imprisonment upto 3 years or fine upto Rs 2 lakh or both</td>
</tr>
<tr>
<td>2</td>
<td>66</td>
<td>Computer related offences</td>
<td>Imprisonment upto 3 years or fine upto Rs 5 lakh or both</td>
</tr>
<tr>
<td>3</td>
<td>66A</td>
<td>Sending offensive messages through communication device</td>
<td>Imprisonment upto 3 years and fine</td>
</tr>
<tr>
<td>4</td>
<td>66B</td>
<td>Dishonestly receiving the stolen computer resource and communication device</td>
<td>Imprisonment upto 3 years or fine upto Rs. 1 lakh</td>
</tr>
<tr>
<td>5</td>
<td>66C</td>
<td>Theft of identity</td>
<td>Imprisonment upto 3 years and fine upto Rs. 1 lakh</td>
</tr>
<tr>
<td>6</td>
<td>66D</td>
<td>Cheating by personation by using computer resource or communication device</td>
<td>Imprisonment upto 3 years and fine upto Rs. 1 lakh</td>
</tr>
<tr>
<td>7</td>
<td>66E</td>
<td>Violation of privacy</td>
<td>Imprisonment upto 3 years or fine upto Rs. 1 lakh or both</td>
</tr>
<tr>
<td>8</td>
<td>66F</td>
<td>Cyber terrorism</td>
<td>Life imprisonment</td>
</tr>
<tr>
<td>9</td>
<td>67</td>
<td>Publishing or transmitting obscene material in e-form</td>
<td>Upon 1st conviction with imprisonment upto 3 years and fine upto Rs 5 lakh; and upon 2nd or subsequent conviction with imprisonment upto 5 years and fine upto Rs 10 lakh.</td>
</tr>
<tr>
<td>10</td>
<td>67A</td>
<td>Publishing or transmitting material containing sexually explicit act in e-form</td>
<td>Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.</td>
</tr>
<tr>
<td>11</td>
<td>67B</td>
<td>Publishing or transmitting material depicting children in sexually explicit act etc. in e-form</td>
<td>Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.</td>
</tr>
<tr>
<td>12</td>
<td>67C</td>
<td>Violating the directions to preserve and retain the information by intermediaries</td>
<td>Imprisonment upto 3 years and fine</td>
</tr>
</tbody>
</table>

*Ibid., Section 78*
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>68</td>
<td>Violating the directions of Controller by Certifying Authority or his employee</td>
<td>Imprisonment upto 2 years or fine upto Rs 1 lakh or both</td>
</tr>
<tr>
<td>14.</td>
<td>69</td>
<td>Violating the directions of the Central Government or State Government to a subscriber to extend facilities to decrypt information</td>
<td>Imprisonment upto 7 years and fine</td>
</tr>
<tr>
<td>15.</td>
<td>69A</td>
<td>Violating the directions to block any information for access by the public</td>
<td>Imprisonment upto 7 years and fine</td>
</tr>
<tr>
<td>16.</td>
<td>69B</td>
<td>Violating the directions to monitor and collect traffic data or information</td>
<td>Imprisonment upto 3 years and fine</td>
</tr>
<tr>
<td>17.</td>
<td>70 &amp; 70A</td>
<td>Unauthorized access to a computer system</td>
<td>Imprisonment upto 10 years and fine</td>
</tr>
<tr>
<td>18.</td>
<td>70B</td>
<td>Violating the directions of the Indian Computer Emergency Response Team (CERT-IN)</td>
<td>Imprisonment upto 1 years or fine upto Rs 1 lakh or both</td>
</tr>
<tr>
<td>19.</td>
<td>71</td>
<td>Penalty for misrepresentation</td>
<td>Imprisonment upto 2 years or fine upto Rs 1 lakh or both</td>
</tr>
<tr>
<td>20.</td>
<td>72</td>
<td>Penalty for breach of confidentiality and privacy</td>
<td>Imprisonment upto 2 years or fine upto Rs 1 lakh or both</td>
</tr>
<tr>
<td>21.</td>
<td>72A</td>
<td>Disclosure of information in breach of lawful contract</td>
<td>Imprisonment upto 3 years or fine upto Rs 5 lakh or both</td>
</tr>
<tr>
<td>22.</td>
<td>73</td>
<td>Penalty for publishing electronic signature certificate false in certain particulars</td>
<td>Imprisonment upto 2 years or fine upto Rs 1 lakh or both</td>
</tr>
<tr>
<td>23.</td>
<td>74</td>
<td>Publication for fraudulent purpose</td>
<td>Imprisonment upto 2 years or fine upto Rs 1 lakh or both</td>
</tr>
</tbody>
</table>

### L. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

An intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.\(^{246}\) However, the following conditions must be fulfilled –

(i). 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

(ii). The intermediary does not –

\(^{246}\) *Ibid., Section 79 (1)*
a. Initiate the transmission,
b. Select the receiver of the transmission, and
c. Select or modify the information contained in the transmission;

(iii). The intermediary observes due diligence while discharging his duties under this Act & observes such other guidelines as the Central Govt. may prescribe in this behalf.\textsuperscript{247}

However, the intermediary shall be liable 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.\textsuperscript{248}

‘Third party information’ means any information dealt with by an intermediary in his capacity as an intermediary.\textsuperscript{249}

M. EXAMINER OF ELECTRONIC EVIDENCE

For the purposes of providing expert opinion on electronic form evidence before any court or other authority, the Central Government may specify, by notification in the Official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.\textsuperscript{250}

‘Electronic form evidence’ means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.\textsuperscript{251}

N. REVIEW: GREY AREAS OF THE INFORMATION TECHNOLOGY ACT, 2000

Information technology has played very important role in the lives of people. Paper based communication has been substituted by e-communication and also we

\textsuperscript{247} Ibid., Section 79 (2)
\textsuperscript{248} Ibid., Section 79 (3)
\textsuperscript{249} Ibid., Explanation to Section 79 (3)
\textsuperscript{250} Ibid., Section 79 A
\textsuperscript{251} Ibid., Explanation to Section 79A
have new concepts such as e-governance, e-commerce, e-banking, e-contract and so on. We can interact with anyone, anywhere and everywhere in no time. We can find valuable information while sitting at home.

Despite the various advantages, the Information Technology Act, 2000 has the following grey areas:

1. **Jurisdiction**
   
   Cyber jurisdiction or jurisdiction in cyberspace refers to a real world government’s power and a normally existing court’s authority over internet users and their activities in the cyber world. However, the IT Act does not cover the important issue of jurisdiction which is very important legal aspect in deciding the place of filing the case.

2. **E-mail authenticity or its evidentiary value**
   
   IT Act does not touch e-mail authenticity or its evidentiary value in the hands of receiver.

3. **Intellectual Property Rights**
   
   Though proviso to section 81 which is incorporated by the IT (Amendment) Act, 2008 provides that this Act shall not restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patent Act, 1970, but does not contain special provisions for protection of IPRs such as copyrights, trademarks, patents etc. in digital medium.

4. **Domain name infringement**
   
   The concept of e-commerce is mainly based upon domain name. However, this Act is silent about the domain names infringement, cyber squatting, typo-squatting, spamming and security of information at various levels.

5. **Cross-border tax**
   
   In the era of globalization, international trade and taxation policies are very important. However, this Act does not talk about the cross-border taxation policy at the international level when the international contract is signed online.

6. **Failure to surrender licence is a non-cognizable offence**
   
   According to section 33 of the IT Act, 2000 when licence of the certifying authority is suspended or revoked then he must immediately surrender his licence to controller. However, where such certifying authority fails to surrender licence then he
shall be guilty of an offence and shall be punished with imprisonment which may extend up to 6 months or a fine which may extend to Rs. 10,000 or both.

Further, u/s 77B, which is incorporated by the IT (Amendment) Act, 2008 any offence punishable with imprisonment of 3 years or above shall be cognizable. Therefore, failure to surrender licence u/s 33 is a non-cognizable offence.

However, licence is backbone of digital/electronic signature certificates because only licenced CA can issue digital/electronic signature certificates, therefore, where a CA whose licence has been revoked or suspended if fails to surrender his licence then it should be a cognizable offence.

7. **Intermediary without directions**

Under section 79 as amended by the IT (Amendment) Act, 2008 it is provided that “where any intermediary 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 any unlawful act and the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner, then he is liable under this Act.”

However, u/s 79 no directions are given to intermediary to install any appropriate software so as to prevent transmission of obscene or pornographic material or any infringed material. Therefore, intermediary must be given effective directions for ensuring installation of appropriate software for preventing pornographic or obscene material being transmitted over their networks and protection against viruses. Their liability must be decided strictly.

8. **Only broad kind of cyber crimes and contraventions are covered**

The IT Act, 2000 covers only broad kind of cyber crimes and contraventions. There were only 10 offences initially under the IT Act, 2000. However, increased use of technology by the criminals made it necessary to increase the number of cyber offences under this Act. Accordingly, by the IT (Amendment) Act, 2008, 13 new cyber offences were inserted whereas 7 existing offences were substituted. It is important to note that various crimes like cyber stalking, violating privacy of a person, cyber terrorism, receiving and retaining computer resource and offences
against computer are made punishable by the IT (Amendment) Act, 20078. Further, using communication device for committing any offence is also punishable.

However, following loopholes regarding cyber offences are still there:

a. The term cyber crime and cyber offence as such is not defined under IT Act, 2000.
b. Offences mentioned under Chapter 13 are not exhaustive.
c. No illustration or examples of such offences are given.
d. Some offences like chatroom abuses, watching porno websites are still not covered.

9. **Important documents such as power of attorney etc. are not covered**

Another loophole of the IT Act, 2000 is that it is not applicable to various documents covered under Schedule I. However, important documents such as power of attorney, will, trust, any contract of sale of immovable property and a negotiable instrument are mentioned under Schedule I, hence not covered under the IT Act, 2000. Therefore, where e-contract relating to immovable property is formed or will is made in electronic form, then the IT Act shall not be applicable.

10. **Statutory bodies may not accept electronic documents**

Statutory bodies are not bound to accept electronic documents under the IT Act, 2000. It is significant to note that section 9 is the biggest loophole of the IT Act, 2000. On one hand, the main aim and objective of the IT Act, 2000 was to facilitate e-governance, however on the other hand, section 9 provides that no one can insist any government office to interact in electronic form.

However, one view for introducing section 9 may be that during this transitional period government offices would take some time to keep pace with technology. The IT Act was enacted in 2000 and almost one decade is over, now it is high time to implement this Act by providing sufficient training to government and police officials and accordingly section 9 should either be abolished or diluted and it should be made compulsory for government bodies to accept electronic documents.

11. **No parameter for implementation**

This Act does not lay down any parameters for its implementation. In India, government and police officials are not computer or technology expert. Even Judges
are not fully sensitized to technology. Therefore, question of implementation of IT Act, 2000 does not arise.

Therefore, for proper implementation of this Act, there must be sensitization of Judiciary, prosecution and police officials to the technology.