Chapter IV

Indian Law Regime to Combat Cyber Crime
Estelar
CHAPTER – IV

INDIAN LAW REGIME TO COMBAT CYBERCRIME

The evolution of law can be historically traced back from the origin of civil society. With the gradual development of society, people started living and working together, forming groups which eventually led to the formation of the State. There was need for regulating the conducts of individuals inter se; therefore, State formed the rules of governance which later came to be known as ‘law’. Thus development of law is a process which continues with the changes and advancement in the social circumstances. Law is generally made to meet the needs of the society and therefore, it is a dynamic concept which undergoes changes with changing needs of the society. The modern technological evolution has enabled human society to prosper and progress but at the same time has given rise to new problem which were hitherto not known to mankind and cyber criminality is one such grey area which emerged only a few decades ago. The tremendous progress made by computer technology during the last quarter of the 20th century has now made it possible for the people to visually chat, send messages, transmit information and conduct business with a person in any part of the world through internet. The computer as an innovative mechanism has increased our capacity to store, search, retrieve, and communicate data as also accessibility to information which has made it possible for us to communicate with any person, anywhere, anytime in the world.¹

NEED FOR A CYBER LAW

The information technology advanced by computer network undoubtedly pervades every aspect of society and governance in the present new millennium. With the increased dependence of e-commerce and e-governance, a wide variety of legal issues related to use of internet as well as other forms of computer or digital processing devices such as violation of intellectual property, piracy, freedom of expression, jurisdiction etc. have emerged, which need to be tackled through the instrumentality of law. Since cyberspace has no geographical limitations or boundaries nor does it have any physical characteristics such as sex, age, etc., it poses a big challenge before the law enforcement agencies for regulating cyberspace transactions of citizen within a country’s territorial jurisdiction. 2 Though in practical terms, an internet user is subject to the laws of the State within which he/she goes online but this general rules into conflict where the dispute are international in nature. It is true that at the time when computer technology was at its developing stage, no one ever contemplated that it can be indiscreetly misused by the internet users for criminal purposes. Because of the anonymity of its character and least possibility of being detected, the cyber criminal are misusing the computer for a variety of crimes which calls for the need for an effective legal framework and regulatory measures to prevent the incidence of this peculiar type of criminality which is rampant in cyberspace.

International law is a primary concern of the United Nations. The mandate for the activities in the field emanates from the Charter of the United Nations which, in its Preamble, set the goal ‘to establish conditions under which justice and respect for the obligations arising from treaties and other source of international law can be maintained’. The International

2 Ibid.
Court of justice, located in The Hague (Netherlands), is one of the six major organs of the United Nations. The Court, in existence since 1946 serves as the successor to the Permanent Court of the International Justice established by the League of Nations; and derives its authority from a statute which forms an integral part of the charter of the United Nations. The Court has two functions: to render judgments on disputes submitted to it by states, and to furnish advisory opinions on questions referred to it by authorized bodies.3

The International Law Commission was established by the United Nations General Assembly4 resolution of Nov 21, 1947. Its primary objective is the ‘promotion of progressive development of international law and its codification’.5 The statute has been amended by the General Assembly a number of times has updated text of which is available online. The commission meets in the one annual session in Geneva and reports to the General Assembly.

The United Nations Commission on International Trade Law (UNCITRAL) was established by the General Assembly Resolution6 of December 17, 1996. Section I and II of the Resolution define the power and functions of the Commission. Its primary objective is the ‘promotion of the progressive harmonization and unification of the law of the international trade’.7 The Commission meets in one annual session, convened alternately in New York (even years) and Vienna (odd years), and reports to the General Assembly.

Amidst growing concern for regulation of electronic commerce and to evolve standards which could be adopted as guidelines by the states

4 Resolution 174 (II) of Nov 21 1947.
5 Article 1 of the Statue
6 Resolution 2205 (XXI) of December 17, 1996.
7 Section 1 of the Resolution of December 17, 1996.

{182}
concerned in framing domestic laws on the subject, the UNCITRAL adopted a resolution on ‘Legal Value of Computer Records’, which was approved through a resolution on December 11, 1985 by the United Nations General Assembly. This was followed by the ‘Model law on Electronic Commerce’ which was accepted by the United Nations general Assembly through a resolution on 30th January 1997. The resolution obliges the member nations to give proper consideration to the provisions of the model law framing or revising (as the case may be) their law with a view to achieve uniformity of law on this point. Moving further in this direction the UNCITRAL adopted a ‘Model law on Electronic Signatures’ which was adopted through a resolution by the United Nations general Assembly on December 12, 2001.

With the globalization of trade and commerce, international business contracts between various governments or between corporate houses of different nations had become very natural. This, however, could not be accomplished electronically unless the offers, acceptances and the communications between the parties through electronic means were accorded legal sanctity. To facilitate this, another UN initiative was taken in the year 2005 in the form of United Nations Convention on the Use of Electronic Communications in international Contracts.

In the year 2007 the UNCITRAL came out with a document that identified main legal issues coming in the way of promoting international trade through electronic means and dealt with various aspects of these issues with a view to smoothen the process of international trade. This document was published in the year 2009 entitled ‘Promoting Confidence in Electronic Commerce; Legal Issues on International use of Electronic Authentication and Signature Methods’. It is a reference document and is in the form of standalone publication. It is turn also expected to help
UNCITRAL identify the areas where it may pursue harmonization activities in future.  

a. Information Technology and India

Responding to aforementioned initiative, India drafted her first law on electronic commerce; the Electronic Commerce Act, 1998 with Electronic Commerce Support Act, 1998. It recalled the rapid development of information and communication technologies revolutionizing the business practices; the transactions accomplished through electronic means-collectively “electronic commerce” – creating new legal issues; the shift paper-based to electronic transactions raising question concerning recognition, authenticity and enforceability of electronic documents and signatures; and the challenge before lawmaker of striking a balance between conflicting goals of safeguarding electronic commerce and encouraging technological development.

Statutory Law Foundations of Cyber Law

The law regime of cyber law comprises the Information Technology Act, 2000, Indian Penal Code, 1860, Indian Evidence Act, 1872, Criminal Procedure Code, 1973, the Bankers’ Book Evidence Act, 1891, the Reserve Bank of India Act, 1934. Since the Indian Penal Code is the substantive criminal law of the country which was drafted centuries ago when even the computers were not in existence, therefore, the code deals with only the traditional crimes. In order to attune the Code with the genesis of the cyber crime and to encompass the cyber crimes within its ambit necessary amendments were introduced in the Code to make it effective in support of the I.T. Act. Similarly necessary amendments have also been introduced in the Indian Evidence Act to take note of the documents which are preserved in the computer system and its accessories

so that they can be admissible in evidence during the course of the trial. These different enactments are being dealt hereunder:

b. INFORMATION TECHNOLOGY ACT, 2000:

Historical Genesis of the I.T, Act, 2000:

The Electronic Commerce Act, 1998 aimed at ‘facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions, the use of digital signatures and other issues related to electronic commerce’. Another draft known as Electronic Commerce Support Act, 1998 had eight sections which were mainly concerned with necessary amendments to other Acts to bring the latter in complete harmony with Electronic Commerce Act, 1998.

The above drafts had been prepared by the Ministry of Commerce. Parallel drafts had also been prepared by the Department of Electronics. Out of these four drafts the Law Ministry had to make a final Draft and to put it before Parliament.

However, with the birth of the Ministry of Information Technology, the job was undertaken by it, and what came forth was the Information Technology Bill, 1999. The Bill was introduced in Parliament in December 1999, was passed in May, 2000, and got the Presidential assent on June 09, 2000. It came into effect from October 23, 2000.

Scheme of the Information Technology Act, 2000:

The Act totally has 13 chapters and 90 sections (the last four sections namely section 91 to 94 in the ITA 2000 dealt with the amendments to the

---

four acts namely, the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker’s Book Evidence Act 1891 and the Reserve bank of India 1934).

**Applicability of the IT Act, 2000:**

The act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person.

**Object of the IT Act, 2000**

The electronic transactions like other parts of the globe, are in vogue in India, however they were without legal sanctity before the enactment of IT Act, 2000.\(^\text{12}\) The increasing growth of electronic commerce, popularly called e-commerce, made it necessary to have legal protection to such transaction. The Indian Parliament took a step of seminal importance by passing the Information Technology Act, 2000.\(^\text{13}\) This Act seeks to achieve various objects, which are discussed succinctly as under:

1. To respond and give effect to the United Nations’ call to all States to give favourable consideration to Model Law when they enact or revise their laws so as to facilitate harmonization of the laws governing alternatives to paper based methods of communication and storage of information.

2. To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly called as “electronic commerce” which involves the use of alternatives to paper based methods of communication and storage of information.

---

\(^{12}\) This fact was admitted by the Parliamentary Affairs Minister Shri Pramod Mahajan in Parliament. (Hindustan Times 16 May, 2000).

\(^{13}\) Farooq Ahmad: Cyber Law In India (Law on Internet), 3rd Edn, 2008, p-34
3. To facilitate electronic filing of documents with the Government agencies so as to promote efficient delivery of government services by means of reliable electronic records.
4. To facilitate electronic storage of data;
5. To facilitate and give legal sanction to electronic fraud transfers;
6. To give legal recognition for keeping books of account by Bankers in electronic form;
7. To amend the Indian Penal code, 1860, the Indian Evidence Act, 1872, the Banker’ Book evidence Act, 1891, and the Reserve Bank of India Act, 1934.

IT Act envisages to provide the legal infrastructure for e-commerce in India and would have a major impact for e-business and the new economy.

Scope of the IT Act, 2000:

The existing laws were framed without envisaging the use of electronic means of communication. Before the adoption of Model Law, general feeling across the nations was that the legal requirement of paper based documentation and communication causes hindrance in the use of modern means of communication. 14 UNCITRAL had two extreme positions to deal with. One created by rigid legislations that do not encompass electronic commerce and the other, by increasing use of transfer and storage of information by electronic means throughout the world but without legal security.

The Model Law represents a compromise of these two extremes by allowing States to adopt their domestic legislation to developments in communication technology applicable to trade law without necessitating

---

14 Farooq Ahmad: Cyber Law In India (Law on Internet), 3rd Edn, 2008, p-35
the wholesale removal of the paper based requirements or disturbing the legal concepts and approaches underlying those requirements. A new approach called “functional equivalent approach” was suggested which is based on an analysis of the purposes and functions of the traditional paper based requirements with a view to determine how those purposes or functions could be fulfilled through electronic commerce techniques.

The courts while interpreting the IT Act have to bear in mind that though the focus is on paperless means of communication, it is not intended, save as otherwise expressly provided in the IT Act, to alter fundamental doctrines and requirements of paper based communications.

The Model Law gives mandate to States to exclude any transaction from the operation of the Act. This may be based on the fact that there are a number of special contracts or instruments so familiar to the public, such as a will, or have become such well established figures of mercantile customs, such as bill of lading, that their manifestation in paper form has become an integral part of their character.\textsuperscript{15}

The Indian Parliament being alive to the ground realities such as lack of infrastructure for new technology, computer literacy and fundamental equivalents decided to limit the scope of the IT Act and did not extend it to\textsuperscript{16}.

(a) A negotiable instrument other than a cheque as defined in Section 13 of the Negotiable Instruments Act, 1881;
(b) A power of Attorney as defined in Section 1A of the Powers of Attorney Act, 1882;
(c) A trust as defined in Section 3 of the Indian Trusts Act, 1882;

\textsuperscript{16} There are some specific exclusion to the Act (i.e. where it is not applicable) as detailed in the First Schedule.
(d) A will as defined in clause 4 of Section 2 of the Indian succession Act, 1925 including any other testamentary disposition by whatever name called;

(e) Any contract for the sale or conveyance of immovable property or any interest in such property;

(f) Any such class of documents or transactions as may be notified by the central Government in the official Gazette.\(^{17}\)

The above documents include disposition of real estate that is commonly required to be in writing almost throughout the Common Law world. These exceptions will not present any impediment to the growth of electronic commerce. The functional equivalents will, with the passage of time, emerge in this area as well and even at present there are clear hints in this direction. For example, Model Law specifically deals with the bill of lading, electronic transfer of payment and the pseudonymous “electronic cheque”.

The IT Act extends to the whole of India, including the state of Jammu and Kashmir and has come into force on 17.10.2000.\(^{18}\) The provision of the IT Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.\(^{19}\) It also applies to any offence or contravention committed outside India by any person irrespective of his nationality if that act or contravention involves a computer, computer system or computer network located in India.\(^{20}\) The extra-territorial ambit of the IT Act is not unusual. The provision giving extra-territorial jurisdiction is found in IT specific

---

17 Section 1(4) of the IT Act, 2000. This provision corresponds with Section 4(1) of the Singapore Electronic Transactions Act, 1988.
18 Vide notification No. GSR 788(E), dated 17-10-2000.
19 Section 81 of the Information Technology Act, 2000.
20 Section 1(2) and 75 of the Information Technology Act, 2000.
legislation of other jurisdiction also.\textsuperscript{21} Obviously the need for such provision is driven by the borderless nature of the Internet. These provisions are, however, viable only if there is mutual co-operation amongst enforcement authorities and Governments.\textsuperscript{22}

The Indian IT Act is unique in many respects. It casts its net very wide. It brings many issues under one umbrella for which legislations have been enacted in other jurisdictions.

The IT Act, \textit{inter-alia}, includes within its ambit legal recognition of electronic records and digital signatures, authentication and retention of electronic records. It accord legal recognition to records, files or document that are retained in an electronic form. It enables public institutions and government departments to issue electronic licences and permits and thus paves the way for electronic governance. It establishes the legal framework that will provide for the setting up of a public key infrastructure. The liability of the service providers for third party content has been clarified. The provision for the appointment, powers and functions of the Controller of the Certifying Authorities and the duties of the subscriber have been provided. This Act also makes offences like tampering with computer source document, hacking and publication of obscene information punishable. A provision for the establishment of special tribunal-Cyber Regulations Appellate Tribunal has also been made.

IT Act 2000 attempts to deal with Cyber crimes. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. Besides this, the Act has also proposed a legal


framework for the authentication and origin of electronic records/communications through digital signature. The implication of these provisions for the e-businesses would be that e-mail would not be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. The legislation throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. It also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signature that would be required to have been passed through a system of a security procedure, as stipulated by the Government of a later date. Now under the Act it shall be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. Finally, the Act gives the legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. 23

Salient Features of Information Technology Act, 2000:

Salient features of IT Act, 2000 are as follows:

a. The Act empowers the government departments to accept filing, creating and retention of official documents in the digital format. The Act also put forward the proposal for setting up the legal framework essential for the authentication and origin of electronic records/communications through digital signature.

b. The Act legalizes the e-mail and gives it the status of being valid form of carrying out communication in India. This implies that e-mail can be duly produced and approved in a court of law, thus can be a regarded as substantial document to carry out legal proceedings.

---


{191}
c. The Act also talks about digital signature and digital records. These have been also awarded the status of being legal and valid means that can form strong basis for launching litigation in a court of law.
d. The Act now allows Government to issue notification on the web thus heralding e-governance.
e. It cases the task of companies the filing any form, application or document by laying down the guidelines to be submitted at any appropriate office, authority, body or agency owned or controlled by the government.
f. The Act also provides statutory remedy to the corporate in case the crime against the accused for breaking into their computer systems or network and damaging and copying the date is proven.
g. The Act sets up the Territorial Jurisdiction of the Adjudicating Officers for Cyber crimes and Cyber Regulation Appellate Tribunal.
h. The Act has also laid guidelines for providing Internet Services on a license on a non-exclusive basis.

The IT Act is a pioneer act in the field of information technology in India and the only legislation which dedicates itself fully to the electronic situation.\textsuperscript{24} India is the 12\textsuperscript{th} nation in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan.\textsuperscript{25}

**Terminologies defined under Section 2:**

Section 2 defines the various terms occurring in IT Act, 2000 such as access,\textsuperscript{26} addressee,\textsuperscript{27} affixing electronic signature,\textsuperscript{28} appropriate

\textsuperscript{24}Talat Fatima: Cybercrimes, Eastern Book Company, 1st Edn. 2011, p-458
\textsuperscript{26}Section 2(a) of the Information Technology Act, 2000.
\textsuperscript{27}Section 2(b) of the Information Technology Act, 2000.
\textsuperscript{28}Section 2(d) of the Information Technology Act, 2000.
Government,\textsuperscript{29} asymmetric crypto system,\textsuperscript{30} communication device,\textsuperscript{31} computer,\textsuperscript{32} computer network,\textsuperscript{33} computer resource,\textsuperscript{34} computer system,\textsuperscript{35} data,\textsuperscript{36} digital signature,\textsuperscript{37} electronic form,\textsuperscript{38} electronic record,\textsuperscript{39} function,\textsuperscript{40} information\textsuperscript{41} etc.

**Authentication of Electronic Records:**

Section 3 gives legal recognition to electronic records and digital signatures. The section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The Act will enable anybody to verify whether the electronic record is retained intact or has been tempered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

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

a. to derive or reconstruct the original electronic record from the has result produced by the algorithm;

\textsuperscript{29} Section 2(e) of the Information Technology Act, 2000.
\textsuperscript{30} Section 2(f) of the Information Technology Act, 2000.
\textsuperscript{31} Section 2(ha), Inserted by Information Technology (Amendment) Act, 2008.
\textsuperscript{32} Section 2(i) of the Information Technology Act, 2000.
\textsuperscript{33} Section 2(j) of the Information Technology Act, 2000.
\textsuperscript{34} Section 2(k) of the Information Technology Act, 2000.
\textsuperscript{35} Section 2(l) of the Information Technology Act, 2000.
\textsuperscript{36} Section 2(o) of the Information Technology Act, 2000.
\textsuperscript{37} Section 2(p) of the Information Technology Act, 2000.
\textsuperscript{38} Section 2(r) of the Information Technology Act, 2000.
\textsuperscript{39} Section 2(t) of the Information Technology Act, 2000.
\textsuperscript{40}Section 2(u) of the Information Technology Act, 2000.
\textsuperscript{41} Section 2(v) of the Information Technology Act, 2000.
b. that two electronic records can produce the same hash result using the algorithm.

**Electronic Governance**\(^{42}\):

It deals with legal recognition of electronic records and ‘electronic signatures’\(^ {43} \).

Section 4 provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is an electronic form.

Section 5 envisages that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Section 6 provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any licence or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Section 7 envisages that the documents, records or information which to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

a. the information therein remains accessible so as to be usable subsequently;

b. the electronic record is retained in its original format or in a format which accurately represents the information contained;

---

\(^{42}\) Chapter III of the Information Technology Act, 2000.

\(^{43}\) Substituted from Digital Signature by the ITAA, 2008.
c. the details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

Section 8 provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form.

Section 9 envisages that the conditions stipulated in Sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central Government or the State Government.

Section 10 provides that the Central government, in respect of ‘Electronic Signature’ may prescribe by rules as under:

a. the type of electronic signature;
b. the manner and format in which the electronic signature shall be affixed;
c. the manner and procedure which facilitates identification of the person affixing the electronic signature;
d. control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payment; and
e. any other matter which is necessary to give legal effect to electronic signature.

**Attribution, Receipt and Despatch of Electronic Records**: Section 11 lays down how an electronic record is to be attributed to the person who originated it.

---

44 Substituted from Digital Signature by the Information Technology (Amendment) Act, 2008.
Section 12 says down for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made.

Section 13 says down for the manner in which the time and place of despatch and receipt of electronic record sent by the originator shall be identified.

For the purpose of section 13\textsuperscript{46}-

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

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

c. “usual place of residence”, in relation to a body corporate, means the place where it is registered.

**Security Procedure\textsuperscript{47}**: Security procedure deals with security of electronic records and electronic signatures. Section 14 envisages that where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. Section 15 envisages for the security procedure to be applied to electronic signature for being treated as a secure electronic signature. Section 16 envisage for the power of Central Government to prescribe the security procedure in respect of secure electronic records and secure electronic signatures.

\textsuperscript{46} Section 13, sub-section 5 of the Information Technology Act, 2000.
\textsuperscript{47} Chapter V of the Information Technology Act, 2000.
Authorities under the Information Technology Act, 2000

The IT Act, 2000\(^{48}\) in order to give impetus to the electronic activities and to secure electronic signatures, devises the ways and means to achieve reliability in this regard. Thus, it envisages its own legal infrastructure to ensure trustworthy relations online. As clear from above, this is done by establishing a public key Infrastructure in which hierarchy of authorities is its main feature.

Certifying Authorities\(^{49}\) can be termed as the backbone of ‘PKI’\(^{50}\). They are like a hyphen which joins, a buckle which fastens the subscriber to the Controlling Authority. They originated as Trusted Third Parties (TTPs) and are primarily instrumental in cryptographic key management, identification of a party to a transaction. They lend authenticity to the electronic signature, thereby making the electronic message, public keys reliable. Electronic certificates are messages they are signed with the Certification Authority’s private key. It is a trusted member of the PKI family and has power not only to issue the Electronic Signature Certificate but also to revoke the same. A Certifying authority can be generically defined as an authority who shall shoulder the following responsibilities:\(^{51}\)

1. Reliable identification of the persons applying for (signature) key certificates;
2. Verification of legal capacity of the applicants;
3. Confirming the attribution of a public signature key to an identified physical person by way of a signature key certificate;

\(^{48}\) Chapter VI of the Information Technology Act, 2000.
\(^{49}\) Section 2(g) of the IT Act, 2000: “Certifying Authority” means a person who has been granted a licence to issue a Electronic Signature Certificate under section 24 of the IT Act.
\(^{50}\) PKI stands for Public Key Infrastructure.
4. Maintaining the online access to the signature key certificates with the agreement of the signature key owner; and

5. Take measures for the guaranteed confidentiality of a private signature key.

Thus, if a person wants to be sure that a public key belongs to a real person, the person to whom he intends to deal with then to be rest assured, he will have to rely on the identity certificate issued by a trusted Certification Authorities. The IT Act has woven the Certifying Authorities into the PKI and has made them subordinate to the Controlling Authorities. Keeping in mind the importance of the Certifying Authorities in the PKI, it is also important to make the position of the Certifying Authority a promising one. To achieve this, Certifying Authority must have the following attributes:

1. It must have independence and should work without unnecessary restrictions;

2. Internal security is absolutely necessary for the Certifying Authority;

3. Viability and stability must be maintained as evidentiary needs may arise after a long gap of time;

4. There should be existence of a contingent plan;

5. Expertise and knowledge in the technology of encryption and decryption;

6. Securing its own private key;

7. Must be equipped with revocation procedures;

8. Insurance;

---

9. Interaction with foreign certification authorities; and

10. Personal selection and reliable management.

Thus, it is evident that the IT Act has well equipped the Certifying Authority.  

**Controlling Authorities and their Appointment:**

Section 17 empowers the Central Government to appoint a Controller of Certifying Authorities and also appoint such number of Deputy Controllers, Assistant Controllers, other officers and employees as it deems fit. Such appointment is to be notified in the Official Gazette. The controller is at the apex of the PKI. The Controller shall be subject to the general control and directions of the Central Government in respect of the functions which he has to perform under the IT Act, the Deputy Controllers, Assistant Controllers and other officers and employees shall be under the control and general supervision of the Controller.

The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

The Head office of the Controller shall be located as such place as the Central Government may specify. There may be branch offices of the office of the Controller and their place of location shall be notified by the Central Government. The office of the Controller shall have a seal.

---

54 S. 17 amended by the IT (Amendment) Act, 2008 (10 of 2009) by which the words “other officers and employees” has been inserted.
55 Section 17(1)(2)) of the Information Technology Act, 2000.
Functions of Controller:

The Controller empowers the Certifying Authorities by issuing licence to them to issue Electronic Signature Certificate. The controllers enjoy superintendence over the Certifying Authorities.

IT Act enumerates the following functions of controller:\(^{57}\):

a. The controller shall exercise supervision over the activities of the Certifying Authorities.
b. He shall certify public keys of the Certifying Authorities.
c. He shall lay down standard to be maintained by the Certifying Authorities.
d. The Controller shall also lay down the qualification and experiences of the employees of the Certifying Authorities.
e. The conditions on which the Certifying Authorities would conduct their business shall be laid down by the Controller.
f. Specifying the contents of written, printed or visual advertisements that may be distributed or used in respect of Electronic\(^ {58}\) Signature Certificates and the public key.

i. The Controller shall also specify the form and content of an Electronic\(^ {59}\) Signature Certificate.

j. The form and manner in which the accounts shall be maintained by the Certifying Authorities are also to be specified by the Controller.

k. The terms and conditions of the appointment of the auditors and the remuneration to be paid to them shall be specified by the Controller.

---

57 Section 18 of the Information Technology Act, 2000.
58 Cl. (f) of S. 18 has been amended by the IT (Amendment) Act, 2008 and the word “digital” has been replaced by the term “electronic”.
59 Cl. (g) of S. 18 has been amended by the IT (Amendment) Act, 2008 and the word “digital” has been replaced by the term “electronic”.

{200}
1. The Controller shall also facilitate the establishment of any electronic system by a Certifying Authorities and regulation of such systems.

m. He shall also specify the manner in which the Certifying Authorities shall conduct dealings with the subscribers.

n. In case of any conflict of interest arising between the Certifying Authority and the subscriber, the Controller shall be the ultimate authority to resolve it.

o. The Controller shall also lay down the duties of the Certifying Authorities.

p. He should also maintain a database containing the disclosures record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Thus, the Controller has a large area of functions which are almost all related to the Certifying Authorities. It is to be noted here that in the unamended Act, the Controller was to be the repository of all Digital Signature Certificates under Section 20 which has now been omitted by the IT (Amendment) Act, 2008.60

Powers of the Controller

The Controller of Certifying Authorities is a chief administrator and acts as a watchdog for the Certifying Authorities.61 In addition to various functions which he has to perform, he enjoys vast powers to ensure strict compliance and efficient functioning of the functionaries under the IT Act.62 The Controller has the following powers.

1. Power to recognize foreign Certifying Authorities.63

---

60 By virtue of S. 13 of the IT (Amendment) Act, 2008, S. 20 of the principal Act shall be omitted.
61 Farooq Ahmad: Cyber Law In India (Law on Internet):, 3rd Edn, 2008, p-104
63 Section 19 of the Information Technology Act, 2000.
2. Power to issue licence for Electronic Signature Certificate.\(^{64}\)

3. Power to renew licence.\(^{65}\)

4. Power to grant or rejection of licence.\(^{66}\)

5. Power to suspend or revoke licence.\(^{67}\)

6. Power to publish notice of suspension or revocation of licence.\(^{68}\)

7. Power to delegate.\(^{69}\)

8. Power to investigate contraventions\(^{70}\): by virtue of this provision, Controller can exercise the following powers.
   a. Power regarding discovery and production of evidence, etc.
   b. Power of search and seizure.
   c. Power to requisition books of account, etc.
   d. Power to call for information.
   e. Power of survey.
   f. Power to control certain information.
   g. Power to inspect register of companies.

9. Power to have access to computer and data\(^{71}\)

10. Power to issue directions.\(^{72}\)

11. Power to decrypt information.\(^{73}\)

---

64 Section 21 of the Information Technology Act, 2000.
68 Section 26 of the Information Technology Act, 2000.
69 Section 27 of the Information Technology Act, 2000.
70 Section 28 of the Information Technology Act, 2000.
72 Section 68 of the Information Technology Act, 2000.
73 Section 69 of the Information Technology Act, 2000.
The Controller of Certifying Authority also has a power to make regulations consistent with IT Act and the rules made thereunder to carry out the purpose of this Act. The Controller shall also maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority.

**Penalties and Compensation**

**Penalties:** According to the Black’s Law Dictionary\textsuperscript{74} penalty stands for the punishment imposed on a wrongdoer, usually in the form of imprisonment or fine; and, especially, a sum of money exacted as punishment for either a wrong to the state or a civil wrong (as distinguished from compensation for the injured party’s loss). Usually imposed for crimes, penalties are sometime also imposed for civil wrong.

It may be added that with the penalty there is a hidden message from the state to punish the wrongdoer, whereas the compensation is awarded with a view to provide relief to the aggrieved. Thus it may appear that deterrence is the object of imposition of penalty; while the award of compensation is dominated by sense to heal the legal injury suffered by the victim.

1. **Penalty and compensation for damage to computer, computer system etc.\textsuperscript{75}:** If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, accesses or downloads any data, or introduces any computer contaminant, or damage. Or disrupts, or denies access to any person authorised to access, or assists any unauthorised person to access, or to a computer, computer system or computer network in contraventions of the provisions of this Act, rules or regulations made there under; or

\textsuperscript{74} Eighth Edition, 2004, at pp. 3588-89.s
\textsuperscript{75} Section 43 of the Information Technology Act, 2000.
destroys the information residing in, or steals the source code of, or charges the service availed of by a person to the account of another person by tampering with any computer, computer system, or computer network; he shall be liable to pay damage by way of compensation to the person so affected.

2. **Compensation for failure to protect data**76: 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 practice and procedures and thereby causes wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

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

---

76 Section 43 A of the Information Technology Act, 2000.
3. **Penalty for failure to furnish information, return, etc.**

If any Person who is required under the Act to furnish any document or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to penalty not exceeding one lakh and fifty thousand rupees for each such failure. If he is required under the Act to file any return or furnish any information within a specified time, and fails to file or furnish the same within that time, he shall be liable to penalty not exceeding five thousand rupees for every day during such failure continues. Finally, if he is required under the Act to maintain books of account or records, and fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

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

5. **Recovery of penalty or 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 licence or the electronic signature certificate, as the case may be, shall be suspended till the penalty is paid. Where any contravention has been compounded as above, no proceeding or further proceeding, as the case may be, shall be taken against the personal guilty of such contravention in respect of the contravention so compounded.

---

77 Section 44 of the Information Technology Act, 2000.
78 Section 45 of the Information Technology Act, 2000.
79 ibid.
80 Section 64 of the Information Technology Act, 2000.
6. **Penalty for misrepresentation**: Whoever makes any representation to, or suppresses any material fact from, the Controller and the Certifying Authority for obtaining any licence or electronic signature certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

7. **Penalty for breach of confidentiality and privacy**: Any person who, in pursuance of any of the powers conferred under this Act, has secured access to any electronic record without the consent of the person concerned, disclose the same to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

8. **Penalty for publishing false electronic signature certificate**: No person shall publish an electronic signature certificate or otherwise make it available to any other person with the knowledge that (a) the Certifying Authorities listed in the certificate has not issued it; or (b) the subscriber listed in the certificate has not accepted it; or (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation. Any person who contravenes this provision shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

---

81 Section 71 of the Information Technology Act, 2000.
82 Section 72 of the Information Technology Act, 2000.
Adjudication

Power to Adjudicate\(^{84}\):

Section 46 deals with the appointment, powers and functions of adjudicating officer.

**Adjudicating Officer**

The contraventions of any rule, regulation, direction or order made thereunder by a person which renders him liable to pay penalty or compensation\(^{85}\) under the IT Act, are adjudicated upon by an officer appointed by the Central Government. A person to be appointed as an adjudicating officer must possess such experience in the field of information technology and legal or judicial experience in the field of information technology and legal or judicial experience as may be prescribed by the Central Government.\(^{86}\) Such officer shall not be below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer. The adjudicating officer appointed as such “shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore”.\(^{87}\) For matters valuing beyond the amount of rupees five crores, the jurisdiction shall vest in the competent court.

**Powers of the Adjudicating Officer**

The adjudicating officer appointed under the IT Act shall have all the power of a civil court which are conferred on the Cyber Appellate

\(^{84}\) Section 46 of the Information Technology Act, 2000.

\(^{85}\) The words “which renders him liable to pay penalty or compensation” are inserted by S. 23 of the IT (Amendment) Act, 2008 (10 of 2009)

\(^{86}\) S. 46(3) of the Information Technology Act, 2000.

\(^{87}\) S. 46 (1)(A), inserted by Information Technology (Amendment) Act, 2008.
Tribunal (CAT) under Section 58(2) and also all powers which are envisaged in the amend Section 46(5).

1. All the proceedings before the adjudicating officer shall be judicial proceedings within the meaning of Section 193 and 228 IPC.

It shall be deemed to be a civil court for the purposes of Section 345 and 346 of the Criminal Procedure Code, 1973.

---

88 S. 58(2): The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908.

89 S. 23 of the IT Act (Amendment) Act, 2008 (10 of 2009) inserts cl. (c) to sub-s. 5 of S. 46.

90 S. 193. Punishment for false evidence.-Whoever intentionally gives false evidence in any stage of a judicial proceeding, or fabricates false evidence for the purpose of being used in any storage of a judicial proceeding, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine;

and whoever intentionally gives or fabricates false evidence in any other case, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Explanation 1.- A trial before a Court-material is a judicial proceeding.

Explanation 2.- An investigation directed by law preliminary to a proceeding before a Court of Justice, is a stage of judicial proceeding, though that investigation may not take place before a Court of justice.

91 S. 228. Intentional insult or interruption to public servant sitting in judicial proceeding.- Whoever intentionally offers any insult, or cause any interruption to any public servant, while such public servant is sitting in any stage of a judicial proceeding, shall be punished with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees or with both.

92 S. 345. Procedure in certain cases of contempt.- (1) When any such offence as is described in Ss. 175, 178, 179, 180 or S. 228 IPC is committed in the view or presence of any Civil, Criminal or Revenue Court, the Court may cause the offender to be detained in custody and may, at any time before the rising of the Court on the same day, take cognizance of the offence and, after giving the offender a reasonable opportunity of showing cause why he should not be punished under this section, sentence the offender to fine not exceeding two hundred rupees, and, in default of payment of fine, to simple imprisonment for a term which may extend to one month, unless such fine be sooner paid.

(2) In every such case the Court shall record the facts constituting the offence, with the statement (if any) made by the offender, as well as the finding and sentence.

(3) If the offence is under S. 228 IPC, the record shall now the nature and stage of the judicial proceeding in which the Court interrupted or insulted was sitting, and the nature of the interruption or insult.

93S. 346. Procedure where Court considers that case should not be dealt with under Section 345: (1) If the Court in any case considers that a person accused of any of the offences referred to in S. 345 and committed in its view or presence should be imprisoned otherwise than in default of payment of fine, or that a fine exceeding two hundred rupees should be imposed upon him, or such Court is for any other reason of opinion that the case should not be disposed of under S. 345, such Court, after recording the facts constituting the offence and the statement of that accused as hereinbefore provided, may forward the case to a Magistrate having jurisdiction to try the same, and may require security to be given for the appearance of such person before such magistrate, or if sufficient security is not given shall forward such person in custody to such Magistrate.

(2) The Magistrate to whom any case is forwarded under this section shall proceed to deal with, as far as may be, as it were instituted on a police report.
a. It shall also be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.\textsuperscript{94}

Thus, the adjudicating officer serves as the court of first instance regarding contraventions of the IT Act. It has all the powers of a court and is legally equipped to provide remedy to the aggrieved and punish the offender.

\textbf{Factors to be taken into account by the Adjudicating Officer}\textsuperscript{95}: While adjudging the quantum of compensation of the Adjudicating Officer shall have due regard to the following factors, namely-

\begin{enumerate}
\item [(a)] The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
\item [(b)] The amount of loss caused to any person as a result of the default; and
\item [(c)] The repetitive nature of the default.
\end{enumerate}

\textbf{Cyber Appellate Tribunal (CAT)}

The Act establishes a judicial body to adjudicate upon matters arising within the Act called the CAT. It is a fact-finding and as well an appellate authority.\textsuperscript{96} This is a judicial body meant solely to adjudicate upon the contraventions of the IT Act and also handle prosecution of the cybercrimes. This is a body which acts like a court and has all the powers of a civil court established under the Civil Procedure Code, 1908 relating to recall of records, examination of witnesses, issuing summons and warrant, etc. Appeal is taken from the CAT to the High Court concerned and hence, the body sits between the adjudicating officer and the High Court. The cyber cases whether civil or criminal are new to the legal world

\textsuperscript{94} This clause is the newly added clause by Information Technology (Amendment) Act, 2008.
\textsuperscript{95} Section 47 of the Information Technology Act, 2000.
\textsuperscript{96} Talat Fatima: Cybercrimes, Eastern Book Company, Ist Edn. 2011, p-474
and their area is also global hence, as many provisions of such laws are virgin, the CAT is a pioneer body and all its judgments and rulings would be a trendsetter. The main issues with which the CAT is required to deal with can be succinctly circumscribed as follows:

1. It deals with jurisdictional issues as the cybercrimes are global in nature and are not confined to a particular geographical or political locality.

2. Being trans-border crimes, there is bound to be an intermingling of various national laws in a single case or crime and hence, the CAT is also expected to consider the issues of private international laws while adjudicating the cyber cases.

3. The CAT is established especially for taking cognizance of cyber transactions whether concerned with online dealings of electronic commerce, or with violations of the IT Act itself or with cybercrimes. Thus, the body is burdened with the responsibility of interpreting and evolving the provisions of cyber laws, intellectual property laws and traditional penal laws as well as cybercrime specific laws.

4. The CAT is expected to face a challenge to strike a balance between the interests of the Government and end-users of the Internet. It will help prevent all cyber contraventions and is destined to path-breaking work to check cyber fraud, cybercrime and even cyber terrorism.\(^97\) Thus the Tribunal will go a long way in paving the way for an easier, trustworthy and technology centric adjudication of legal provisions.

---

\(^{97}\) K.G. Balakrishnan, Hon’ble Chief Justice of India while inaugurating a Cyber Tribunal in Delhi on 27-7-2009.
Powers of Cyber Appellate Tribunal:

The CAT shall have the same powers as are vested in a civil court under the Civil Procedure Code, 1908 as follows⁹⁸:

1. Summoning and examining any person on oath;
2. Requiring the discovery and production of documents or electronic records;
3. Receiving evidence on affidavit;
4. Issuing commission for the examination of witnesses or documents;
5. Reviewing its decisions;
6. Dismissing an application for default or deciding it ex parte; and
7. Any other matter which may be prescribed.

Thus, the CAT has been given elaborate powers to deal with the situations arising out of electronic activities online and with contraventions of the IT Act itself.

Constitution of Cyber Appellate Tribunal:

The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal, specifying the matters and places in relation to which the Tribunal may exercise jurisdiction.⁹⁹

Composition of Cyber Appellate Tribunal:

The CAT shall consist of a chairperson and such number of the other Members, as the Central Government may, by notification in the Official Gazette, appoint. The selection of Chairperson and Members of

---

⁹⁸ Section 58(2) of the Information Technology Act, 2000.
the Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.\textsuperscript{100}

The CAT established under the amendment Act shall consist of:

(i) **One Chairperson:** The Chairperson shall be appointed by the Central Government in consultation with the Chief Justice of India. A person to be appointed as the Chairperson must have the qualification to be a Judge of High Court.\textsuperscript{101} However, the amended Act says that the Presiding Officer appointed under the IT Act would continue as the Chairperson of the present CAT. In the selection of the Chairperson and other members of the Tribunal, the Central Government shall consult the Chief Justice of India.\textsuperscript{102}

(ii) **Other Members:**

Such number of other Members, as the Central Government may specify, would comprise the Tribunal. The Members shall be from the following heads:

(a) **Technical Members:**

These Members are to be persons having special knowledge of and professional experience in information technology, telecommunication industry, and management or consumer affairs. They are to be appointed by Central Government.\textsuperscript{103}

(b) **Ordinary Members:**

The qualification of such Members include that he should be in the service of the Central or State Government and has held the post of Additional Secretary for a period of at least one year or the post of Joint

\textsuperscript{100} Section 49 of the Information Technology Act, 2000.
\textsuperscript{101} Section 50(1) of the Information Technology Act, 2000.
\textsuperscript{102} Section 49(2) of the Information Technology Act, 2000.
\textsuperscript{103} Section 50(2) of the Information Technology Act, 2000.
Secretary to the Government of India or equivalent post in the Central or State Government for at least seven years.  

(c) **Judicial Members:**

The Judicial Members shall be appointed by the Central Government from persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for at least one year and a Grade I post of that for a period of at least five years.

(iii) The Chairperson and all the Members by virtue of Rule 12 of the CAT (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009 shall before entering upon the office would take oath of the office and secrecy in Form I and II of the said rules respectively.

(iv) **Other Staff:** The Central Government shall also appoint such officers and employees as it thinks fit to aid the Chairperson. This staff shall Chairperson and their salaries, allowances and other terms and conditions of service shall be prescribed by the Central Government.

**Powers of the Chairperson:**

The Chairperson being a jurist has given power not only to adjudicate upon matters but also to judicially administer the work of the Tribunal. In this regard following provisions are notable:

---

104 Ibid.
106 Rules made by the Central Government in exercise of power under S. 87 read with S. 52 of the IT Act and in supersession of Cyber Regulations Appellate Tribunal (Salary, Allowances & Other Terms and Condition of Service of Presiding Officer and Members) Rules, 2003 vide G.S.R. 778(E), Notification, New Delhi, 27-10-2009, Ministry of Communications & Information Technology (Department of Information Technology).
(a) A bench may be constituted by the Chairperson of the Tribunal with one or two members of such Tribunal as the Chairperson may deem fit;

(b) The Benches of the Tribunal shall sit at New Delhi, and at such other places as the Central Government may, in consultation with the Chairperson of the Tribunal, by notification in the Official Gazette, specify;

(c) The Central government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Tribunal may exercise its Jurisdiction, it will be the decision of the Chairperson to transfer a case or a matter from one Bench to another Bench in case it opines that a matter is to be heard by a large Bench.

(d) The Chairperson can transfer a Member from one Bench to another Bench.

(e) The Chairperson shall also have power of general superintendence and directions in the conduct of the affair of the Tribunal.¹⁰⁹

(f) The Chairperson shall also preside over the meetings of the Tribunal.¹¹⁰

(g) Chairperson will also discharge such powers and functions as it is prescribed from time to time.¹¹¹

(h) The Chairperson shall also allocate business among Benches and also the matter which is to be heard by a particular Bench.¹¹²

---

109 Section 52A of the Information Technology Act, 2000..
110 Section 52A, ibid.
111 Section 52A, ibid.
112 Section 52B of the Information Technology Act, 2000.
(i) The Chairperson is also given the power to transfer a pending case either on the application of parties and notify the other party, or *suo moto* without such notice for disposal by the Bench to which it is transferred.\(^\text{113}\)

(j) The Chairperson is also given the power to decide between two dissenting Members of the Tribunal when such dissenting matter is presented to him under reference. Such decision of the Chairperson shall be given after hearing the points of the dissenting Members and the decision shall be on the basis of the opinion of the majority of the Members.\(^\text{114}\)

**Conditions of service:**

The Chairperson and members of the Tribunal shall hold office for a period of five year or upto the age of 65 years whichever is earlier.\(^\text{115}\) Such Chairperson or member when selected as such shall resign from the government post earlier held by him.\(^\text{116}\) The salary, allowances and other terms and conditions of service including pension, gratuity and other retirement benefits of the Chairperson and the Members would be regulated by the CAT (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009.\(^\text{117}\)

The Chairperson or the Member of the CAT may resign from their office on their own will by sending a notice to the Central Government, subject to the condition that such Chairperson or Member shall continue in

\(^{113}\) Section 52C of the Information Technology Act, 2000.

\(^{114}\) Section 52D of the Information Technology Act, 2000.

\(^{115}\) Section 51(1) of the Information Technology Act, 2000.

\(^{116}\) Section 51(3) of the Information Technology Act, 2000.

\(^{117}\) Rules made by the Central Government in exercise of power under S. 87 read with S. 52 of the IT Act and in supersession of Cyber Regulations Appellate Tribunal (Salary, Allowances & Other Terms and Condition of Service of Presiding Officer and Members) Rules, 2003 vide G.S.R. 778(E), Notification, New Delhi, 27-10-2009, Ministry of Communications & Information Technology (Department of Information Technology).
office upto the expiry of three months or until a new incumbent takes over.\textsuperscript{118}

The office of the Chairperson and the members has been laced with legal and procedural safeguard. The ground of the removal of the Chairperson and the Members are proved misbehavior or incapacity\textsuperscript{119} and it is on these grounds that after an enquiry held by a Judge of the Supreme Court that the Central Government can pass the order of removal. Before removal, the incumbent concerned shall be given an opportunity of being heard and to give his explanation regarding the charges leveled against him.\textsuperscript{120} However, the Central Government formulated Cyber Appellate (Procedure for Investigation or Incapacity of Chairperson and Members) Rules, 2009 to deal with the procedure for removal.

Thus, the removal of the Chairperson or the Member is not an easy procedure but it is done after a high level inquiry to find out the truth before it submits its report.

Once decided by the adjudicating officer the matter is not closed finally. The aggrieved gets further opportunities to challenges his order before the higher judicial bodies. An order based on the consent of parties is not appealable.\textsuperscript{121} Thus, the dissatisfied party gets two chances to take the matter in appeal, firstly before the CAT and second appeal before the High Court concerned.

\textsuperscript{118} Section 54(1) of the Information Technology Act, 2000.
\textsuperscript{119} It is to be noted that the ground removal of the Chairperson and Members are the same as in the case of a Judge of Supreme Court or of the High Court. Article 124(4) says that A Judge of the Supreme Court shall not be removed from his office except by an order of the president passed after an address by each House of Parliament supported by a majority of the total membership of that House and by a majority of not less than two-thirds of the members of that House present and voting has been presented to the President in the same session for such removal on the ground of proved misbehavior or incapacity.
\textsuperscript{120} Section 54(2) of the Information Technology Act, 2000.
\textsuperscript{121} Section 57(2) of the Information Technology Act, 2000.
First Appeal to the Tribunal\textsuperscript{122}: 

Any person aggrieved by an order made by Controller or an adjudicating officer under the Act may prefer an appeal to the Tribunal. However, no appeal shall lie to the Tribunal from an order made by an Adjudicating Officer with the consent of the parties.

Every appeal shall be filed within a period of forty five days from the date on which a copy of the order made by the Controller or Adjudicating Officer is received by the person aggrieved; and it shall be in such form and be accompanied by such fee as may be prescribed. However, the Tribunal may entertain an appeal even after 45 days if it is satisfied that there was sufficient cause for not filing it within that period.

On receipt of an appeal, the Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such order thereon as it thinks fit, confirming, modifying or setting aside the order appealed against. The Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller of Adjudicating Officer.

The appeal filed before the 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 six months from the date of the receipt of the appeal.

Appeals to High Court\textsuperscript{123}: 

Any person aggrieved by any decision or order of the Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Tribunal to him on any question of fact or law arising out of such order.

\footnotesize{122 Section 57 of the Information Technology Act, 2000.}
\footnotesize{123 Section 62 of the Information Technology Act, 2000.}
Procedure of the Cyber Appellate Tribunal\textsuperscript{124}

The CAT shall be guided by the following principles in its working:

1. Rules of natural justice;
2. By the related provisions of the IT Act; and

Thus, Section 58 of the IT Act empowers the Tribunal to lay down not only its own procedure but to also decide the place of its sitting.

1. The Tribunal is free to apply the well-settled rules of Natural Justice which are as follows\textsuperscript{125}:

   A. **The doctrine of bias**- This rule says that “no one shall be a Judge in his own cause”. This upholds the concepts of impartiality and fairness and says that the Presiding Officer shall be free from any prejudices. The Supreme Court held in **G.Sarana v. University of Lucknow**,\textsuperscript{126} that the authority to decide the dispute between opposing parties must be one without bias. This rule of bias is only a principle of conduct and is imposed strictly on the exercise of the judicial or quasi-judicial authorities. In case of bias the actual proof is not necessary and the test is that of a reasonable man.\textsuperscript{127}

   B. **Audi altarem partem**- It is another rule of natural justice which implies right to be heard. The rule has two facets; notice of the case to be met and opportunity to explain. Justice cannot be done unless both the sides are given the opportunity to explain their situations and to use the words of Lord Loreburns, it is “a duty lying upon everyone who decides

\textsuperscript{124} Section 58 of the Information Technology Act, 2000.
\textsuperscript{125} Talat Fatima: Cybercrimes, Eastern Book Company, Ist Edn. 2011, p-482.
\textsuperscript{126} AIR 1967 SC 2428.
something” in the exercise of legal power. This rule cannot be ignored for the sake of the convenience of the authority as Lord Atkin rightly says “convenience and justice are often not on speaking terms’. Thus even though some delay, inconvenience or hardship be suffered by the authority or by anyone, the incriminating material be made known to the accused and he should be given an opportunity to defend himself.

Thus, the CAT while adjudicating upon the cases before it must follow the abovementioned rules of natural justice.

C. Real Justice-There is often one more accepted rule of natural justice which says that justice should not only be done but it should be done in such a material manner that one should feel that justice has been done. In other words, justice should not be an artificial thing only by way of pretension or show but it should be actually done so that the aggrieved feels that justice has been met.

2. The IT Act, wherever possible has also mentioned certain rules which are to be followed by the Tribunal. These facets of procedure before a Tribunal are retrieved from the following sections of the Act:

a. Representation- The appellant has been given option to either plead his appeal personally or he can also take the help and advice of the legal practitioners of his choice.128

b. Limitation- The appeal to be filed before the Tribunal must follow the period of limitation for filing a suit. This is done on the basis of the provisions of the Limitation Act, 1963.129

c. Jurisdiction- The IT Act ousts the jurisdiction of a civil court. Such prohibition is regarding two things; firstly no civil court shall have jurisdiction to hear any suit or proceedings in respect of any matter

129 Section 60 of the Information Technology Act, 2000.
which an adjudicating officer appointed under this Act or the Cat is already empowered to determine\textsuperscript{130} and secondly, no injunction can be granted by any court or authority regarding any action taken by such officer or Tribunal.

3. The Act also provides for some part of the procedure to be followed by the Tribunal. Section 58 also declares that the procedure shall be subject to the rules made by the Central Government. Thus, in exercise of powers,\textsuperscript{131} the Central Government made the rules called the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 (Rules, 2000).\textsuperscript{132} The Rules, 2000 has 28 rules which detail out the procedure of filing the application, the procedure of filing the reply and other appeal related procedures.

**Offences in Information Technology Act**

Chapter XI of the Information Technology Act, 2000 has been entitled “Offences”. Broadly speaking, it deals with various offences done in the electronic format, offences concerning computers, computer system and computer networks, (computer crimes) as also those, which come within the ambit of cybercrimes. The real power of today’s internet is that it is available to anyone with a computer and a telephone line. Internet places in an individual’s hand the power of information and communication. This power is being misused by devious mind for criminal purpose. Cybercrimes constitute one of the most important challenges facing cyberspace today.

Cybercrimes has no one exhaustive definition. Cybercrime refers to all the activities done with criminal intent in cyberspace or using the

\begin{footnotesize}
\textsuperscript{130} Section 61 of the Information Technology Act, 2000.
\textsuperscript{131} Conferred by Section 87 of the Information Technology Act, 2000.
\textsuperscript{132} Vide G.S.R. 791(E), 17-10-2000.
\end{footnotesize}
medium of internet. The IT Act creates several offences and prescribes punishments therefore which are as follows:

1. **Tampering with Computer Source Documents:**

According to Section 65, whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

**Explanation** -

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

2. **Computer Related Offences:**

According to Section 66 of IT Act, if any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

**Explanation:** For the purpose of this section,-

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

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

---

133 Section 65 of the Information Technology Act, 2000.
135 Substituted by Information Technology (Amendment) Act, 2008.
Section 66 is now a widened one with a list of offences after the Information Technology (Amendment) Act, 2008:

3. Punishment for sending offensive messages through communication service, etc.\textsuperscript{136}:

Sending offensive message through communication services, causing annoyance etc through an electronic communication or sending an e-mail to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment upto three years or fine.

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

4. Punishment for dishonestly receiving stolen computer resource or communication device.\textsuperscript{137}

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

5. Punishment for identity theft.\textsuperscript{138}

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other

\textsuperscript{136} Section 66A introduced vide Information Technology (amendment) Act, 2008.
\textsuperscript{137} Section 66B introduced vide Information Technology (amendment) Act, 2008.
\textsuperscript{138} Section 66C introduced vide Information Technology (amendment) Act, 2008.
person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

6. Punishment for cheating by personation by using computer resource.\textsuperscript{139}

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

7. Punishment for violation of privacy.\textsuperscript{140}

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

\textbf{Explanation} - For the purposes of this section--

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

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

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

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

\textsuperscript{139} Section 66D introduced vide Information Technology (amendment) Act, 2008.
\textsuperscript{140} Section 66E introduced vide Information Technology (amendment) Act, 2008.
(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that--

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

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

8. Punishment for cyber terrorism:\textsuperscript{141}

(1) Whoever,-

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

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

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

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

(B) knowingly or intentionally penetrates or accesses a computer resource without 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

\textsuperscript{141} Section 66F introduced vide Information Technology (amendment) Act, 2008.
relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

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

9. Punishment for publishing or transmitting obscene material in electronic form.\(^{142}\)

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

\(^{142}\) Section 67 amended by Information Technology (amendment) Act, 2008..
10. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:\(^{143}\)

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

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

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

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

11. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:\(^{144}\)

Whoever,-

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

---

\(^{143}\) Section 67A introduced vide Information Technology (amendment) Act, 2008.

\(^{144}\) Section 67B introduced vide Information Technology (amendment) Act, 2008.
b. creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
c. cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
d. facilitates abusing children online; or
e. records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

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

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

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

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

**Explanation:** For the purposes of this section, "children" means a person who has not completed the age of 18 years.
12. **Preservation and retention of information by intermediaries**\(^{145}\): It is the duty of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. An intermediary who intentionally or knowingly contravenes this provision shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

13. **Punishment for Disclosure of information in breach of lawful contract**\(^{146}\):

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

14. **Publication for fraudulent purpose**\(^{147}\):

Whoever 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 two years, or with fine which may extend to one lakh rupees, or with both.

---

\(^{145}\) Section 67C of the Information Technology Act, 2000.

\(^{146}\) Section 72A of the Information Technology Act, 2000.

\(^{147}\) Section 74 of the Information Technology Act, 2000.
15. *Punishment for abetment of offences*: 

Whoever abets any offence shall, if the act abetted is committed in consequence of the abatement, and no express provision is made by this Act for the punishment of such abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act. It has given by way of explanation that an Act or offence is said to be committed in consequences of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

16. *Punishment to attempt to commit offences*: 

Whoever attempts to commit an offence punishable by the Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, were no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

17. *Offences by Companies*: If contravention of any provision of the Act or rules or order made there under is committed by a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, the said person in charge of the conduct of the business of the company shall not be liable if he proves that the said

---

149 Section 84C of the Information Technology Act, 2000.  
150 Section 85 of the Information Technology Act, 2000.
contravention took place without his knowledge or that he exercised due
diligence to prevent such contravention.

On the other hand if it is proved that the said contravention has
taken place with the consent or connivance of, or is attributable to any
neglect on the part of any manager, director, secretary or other officer of
the company, such manager, director, secretary or other officer shall also
be deemed to be guilty of the contravention and shall be liable to be
proceeded against and punished accordingly. Here, ‘company’ means
anybody corporate and includes a firm or other association of individuals;
and ‘director’, in relation to a firm, means a partner in the firm.

Extraterritorial Jurisdiction\textsuperscript{151}:

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

Power to investigate offences\textsuperscript{152}:

Power to investigate offences.-Notwithstanding anything contained
in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not
below the rank of ‘Inspector’\textsuperscript{153} shall investigate any offence under this
Act.

\textsuperscript{151} Section 75 of the Information Technology Act.
\textsuperscript{152} Section 78 of the Information Technology Act.
\textsuperscript{153} Substituted from Deputy Superintendent of Police by the Information Technology (Amendment) Act, 2008.
Power of Police Officer:

Section 80 provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central or State Government, if so authorized by the Central Government, may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or is about to commit any offence under this Act.

Section 80 provides that where any person is arrested by an officer other than a police officer, such officer shall immediately send the arrested person to a magistrate having jurisdiction or to the officer in charge of a police station.

Power of Central Government to make Rules:

The Central Government has been authorised under the IT Act to formulate rules to detail out of the provisions of the Act. This is found in two places in the Act; firstly, Section 10 of the Act empowers the Central Government to make rules regarding electronic (digital) signature and under Section 87, there is general power to make rules pertaining to various topics.

a. Power of Central Government to make rules in respect of [Electronic Signature]¹⁵⁴:

The section 10 of the IT Act, 2000 has been amended in 2008 and by virtue of it, the section does away with the term “Digital” and the word “Electronic” has been inserted instead. The section empowers the central government to make rules in respect of the type of electronic signature, the manner and format in which the electronic signature shall be affixed, the

¹⁵⁴ Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
manner which would facilitate identification of the person affixing the electronic signature, the control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments and in respect of any other manner connected thereto with electronic signatures.

ii. Power of Central Government to make general rules:

The Central Government under Section 87 of the IT Act has been given elaborate powers to make rules regarding a number of subjects and provision under the Act. These are as follows:

(1) The Central Government may, by notification in the official Gazette, and in the Electronic Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

155[(a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A;

(aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) f section 3A;

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

---

155 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
(c) the manner and format in which electronic records shall be filed or issued and the method of payment under sub-section (2) of section 6;

156[(ca) the manner in which the authorized service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A.

(d) the matters relating to the type of Electronic Signature, manner and format in which it may be affixed under section 10;

157[(e) the manner of storing and affixing electronic signature creation data under section 15.

(ea) the security procedures and practices under section 16.

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers, 158[Assistant Controllers, other officers and employees] under section 17;

(g) 159[***]

(h) the requirements which an applicant must fulfill under sub-section (2) of section 21;

(i) the period of validity of license granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for license may be made under subsection (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

156 Inserted by Act no. 10 of 2009, w.e.f. 27-10-2009.
157 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
158 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
159 Omitted by Act no. 10 of 2009, w.e.f. 27-10-2009.

{233}
(l) such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a license and the fee payable thereof under section 23;

160[(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35;]

(n) the form in which application for issue of a [Electronic Signature]161 Certificate may be made under sub-section (1) of section 35;

(o) the fee to be paid to the Certifying Authority for issue of a [Electronic Signature]162 Certificate under sub-section(2) of section 35;

163[(oa) the duties of subscribers under section 40A;]

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A;

(p) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;

(r) the salary, allowances and the other terms and conditions of service of the 164[Chairperson and Members] under section 52;

(s) the procedure for investigation of misbehaviour or incapacity of the 165[Chairperson and Members] under sub-section (3) of section 54;

---

160 Inserted by Act no. 10 of 2009, w.e.f. 27-10-2009.
161 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
162 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
163 Inserted by Act no. 10 of 2009, w.e.f. 27-10-2009.
164 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
165 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
(t) the salary and allowances and other conditions of service of other officers and employees under sub-section (3) of section 56;

(u) the form in which appeal may be filed and the fee thereof under subsection (3) of section 57;

(v) any other power of a civil court required to be prescribed under clause (g) of sub-section (2) of section 58; and

(w) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52 A;

(x) the information, duration, manner and form of such information to be retained and preserved under section 67 C;

(y) the procedures and safeguards and interception, monitoring or decryption under sub-section (2) of section 69;

(z) the procedure and safeguards for blocking for access by the public under subsection (2) of section 69 A;

(za) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of section 69 B;

(zb) the information security practices and procedures for protected system under section 70;

(zc) manner of performing functions and duties of the agency under sub-section (3) of section 70 A;

(zd) the officers and employees under sub-section (2) of section 70 (B);

(ze) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70B;

166 Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
(zf) the manner in which the functions and duties of agency shall be performed under sub-section (5) of section 70 B;

(zg) the guidelines to be observed by the intermediaries under sub-section (2) of section 79;

(zh) the modes or methods for encryption under section 84A.

(2) [Every notification made by the Central Government under sub-section (1) of section 70 A and every rule made by it]¹⁶⁷ shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in [***]¹⁶⁸ the rule or both Houses agree that [***]¹⁶⁹ the rule should not be made, [***]¹⁷⁰ the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

**Power of State Government to make Rules:**

The State government may make rules to carry out the provisions of this Act¹⁷¹. These rules may provide for all or any of the following matter, namely:

---

¹⁶⁷ Substituted by Act no. 10 of 2009, w.e.f. 27-10-2009.
¹⁶⁸ Omitted by Act no. 10 of 2009, w.e.f. 27-10-2009., The words “the notification or” omitted by Act 10 of 2009, w.e.f. 27-10-2009.
¹⁶⁹ Ibid.
¹⁷⁰ Ibid.
¹⁷¹ Section 90 of the information Technology Act.
a. The electronic form in which filing, issue, grant, receipt or payment shall be effected under sub-section (1) of Section 6;

b. For matters specified in sub-section (2) of Section 6;

c. Any other matter which is required to be provided by rules by the State Government;

Every rule made by the State Government under this section shall be laid as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, where such legislature consists of one House, before that House.

c. **AMENDMENTS TO CERTAIN STATUTES:**

The Information Technology Act, 2000, to further acceptance and use of documents, evidence and transfer of funds through electronic means, has amended the Indian Penal Code, 1860,\(^1\) the Indian Evidence Act, 1872,\(^2\) the Bankers’ Books Evidence Act, 1891\(^3\) and Reserve bank of India Act, 1934\(^4\) vide the First, Second, Third and Fourth Schedule respectively. The Act has introduced and given legal sanction to electronic record and documents. It permits the use of electronic record in government and its agencies with a view to promote electronic governance. To give a push to electronic contracts, provisions have been made for attribution, acknowledgement and dispatch of electronic records.\(^5\)

---

1. Amendments to the Indian Penal Code:

It is pertinent to point out that the Information Technology Act, 2000 amended various provisions of the Indian Penal Code, 1860. This was done by virtue of section 91 of the Information Technology Act, 2000 which brought various amendments in the Indian Penal Code. These provisions are primarily are offences relating to document. The aim is to also induct ‘electronic record’ thereby making such offences which till now were only paper-based can now also be paperless.

Largely, the amendments to the IPC can be categorized into following headings:

a. Definition: By insertion of Section 29A, the definition of “electronic record” as understood by section 2(1)(t) of the IT Act, 2000 has been introduced in IPC. “Electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer generated micro fiche.

As a result of this amendment all the offences related to documents also include offences related to electronic records which are committed through internet or cyberspace.

b. Offences by or relating to public servants: Section 167 deals with the offence committed by a public servant of framing an incorrect document with intent to cause injury. Consequent to amendment of this section by the IT Act, 2000, now the section also includes electronic records within the term ‘document’. The gist of the offence lies

---

177 According to section 2(1)(t) of the IT Act, 2000.
178 Section 167, Indian Penal Code, 1860.
in the intention of the public servant to cause injury to any person by deviating from his duty.  

\[179\]

c. **Offences of contempt of the lawful authority of public servants:** Chapter 10 of IPC deals with contempt of the lawful authority of public servants and is meant to enforce obedience and respect to their lawful authority. All the amendments made in this Chapter pertains to introduction of ‘electronic record’ by the side of ‘document’ and bringing in par both paper-based and paperless offences. Sections 172,\(^{180}\) 173\(^ {181}\) and 175\(^ {182}\) have been amended to ensure that any action which was done by way of a paper-based document would still be an offence if done by way of electronic means.

\[179\]

d. **Offence relating to evidence:** Sections 192\(^ {183}\) and 204\(^ {184}\) have been amended under the Chapter relating to offences of false evidence and offences against public justice. After the amendments, the offence of fabricating false evidence would also include fabricating of a false electronic record. Likewise, any destruction of an electronic record would attract punishment under section 204.

\[179\]

e. **Offences in relation to document:** The major portion of the amendments made in the IPC is dedicated to the Chapter 18 that is offence relating to documents. All such offence pertaining to and based on the document have been given a wider scope and applicable to electronic record as well. Such amendments primarily relate to use of electronic

---

179 Amended Section -167(IPC) : Public servant framing incorrect document with intent to cause injury.
180 S.172 of the Indian Penal Code: Absconding to avoid service to summons or other proceedings.
181 S.173 of the Indian Penal Code: Preventing service of summons or other proceeding, or preventing publication thereof.
182 S.175 of the Indian Penal Code: Omission to procedure document to public servant by person legally bound to product it.
183 S.192 of the Indian Penal Code: fabricating false evidence.
184 S. 204 of the Indian Penal Code: Destruction of document or electronic record to prevent its production as evidence.
record and affixation of digital signatures for the purpose of forgery. Section 463 which makes forgery a punishable offence has been amended to include forgery by electronic records. Making of a false document under section 464 now includes dishonestly nor fraudulently affixing any digital signature on any electronic record. ‘Affixing digital signature’ has been given the same meaning as assigned to it in section 2(1)(d) of the Act. Sections 466, 468, 470, 471 and 474 have been amended to the same effect that is committing forgery by electronic record and affixing digital signature. It would be interesting to note the amendment made in section 474 is specific. Section 474 can be bifurcated in two parts. Firstly, it makes the possession of any document of the description mentioned in section 466 of IPC knowing the same to be forged and intending to use the same fraudulently or dishonestly as genuine an offence. Second part relates to document of the description mentioned in section 467. However, the IT Act, 2000 has amended only the first part of section 474 and left the second part. The reason being is that the first part being a document described under section 466 deals with a document purporting to be a record or proceeding of or in a court of justice or a public register, etc. The second part being a document described under section 467 deals with will. Since the IT Act, 2000 would not apply to wills at all as excluded by section 1(4)(d), no question of amendments to section 474 with respect to an offence relating to will arises.

Further amendments made in this Chapter pertain to offence of counterfeiting device or mark used for authenticating documents and

185 S. 466 of the Indian Penal Code: Forgery of record of Court or of public register, etc.
186 S. 468 of the Indian Penal Code: Forgery for purpose of cheating.
187 S. 470 of the Indian Penal Code: Forged document or electronic record.
188 S. 471 of the Indian Penal Code: Using as genuine a forged document or electronic record.
189 S. 474 of the Indian Penal Code: Having possession of document described in Ss. 466 or 467, knowing it to be forged and intending to use it as genuine.
190 S. 476 of the Indian Penal Code.
falsification of document.\textsuperscript{191} Electronic record has been included in both the sections.

f. **Criminal Trespass**\textsuperscript{192}: Criminal trespass as an offence has been defined in Section 441 of IPC. In the context of cybercrime, the offence of criminal trespass, generally refers to class of unauthorized access which in computer technology is known as “hacking”. Such an offence when committed shall be punishable with imprisonment for a term which may extend to three months or with fine of five hundred rupees or with both as provided in Indian Penal Code.\textsuperscript{193}

g. **Cheating by Personation**\textsuperscript{194}: The offence of cheating by personation is committed if a person cheats another by pretending to be some other person. E-mail spoofing is the common example of cybercrime which attracts the provision of section 416 of Indian Penal Code.

**Amendment in IPC, 1860 in the ITAA, 2008**: There are also some important amendments in Indian Penal Code, 1860 by the Information Technology (Amendment) Act, 2008.

h. **Amendment in section 4**: In section 4,-

(i) After clause (2), the following clause shall be inserted, namely: “(3) any person in any place without and beyond India committing offence targeting a computer resource located in India;”

(ii) For the Explanation, the following Explanation shall be substituted, namely:

‘Explanation’: In this section-
(a) The word “offence” includes every act committed outside India which, if committed in India, would be punishable under this Code;

(b) The expression “computer resource” shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000.

i. Amendment of section 40: In section 40, in clause (2), the figures and word “118, 119 and 10” shall be inserted.

j. Amendment of section 118: In section 118, for the words “voluntarily conceals, by an act or illegal omission, the existence of a design”. The words “voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design” shall be substituted.

k. Amendment of section 464: In Section 464, for the words “digital signature” wherever they occur, the words “electronic signature” shall be substituted.

2. Amendments to the Indian Evidence Act, 1872:

The law of evidence is the lex fori which governs the Courts. The law of evidence is a part of the law of procedure. Indian Evidence Act, 1872 establishes the rules to be followed by in producing evidence in a court of law. The nature of electronic evidence is such that in almost all cases where any electronic record is to be produced as evidence, it will actually be a copy of the original record that will be exhibited and not the original. Keeping in mind the peculiarities of digital evidence, the Indian Evidence Act, 1872 was amended by the Section 92 of the

---

195 After the figure “117” in clause (2), in section 40.
Information Technology Act, 2000. These amendments as well as can be summarized under following headings:

a. Amendments permitting evidence in electronic form:

   i. In section 3,-

      (a) In the definition of ‘Evidence’ for the words “all document produced for the inspection of the Court”, the word “all document including electronic records produced for the inspection of the Court” shall be substituted;

      (b) After the definition of “India”, the following shall be inserted, namely: ‘the expressions “Certifying Authority”, “digital signature”, “Digital Signature Certificate”, “electronic forms”, “electronic records”, “information”, “secure electronic record”, “secure digital signature” and “subscriber” shall have the same meaning as assigned to them in the Information Technology Act, 2000.

   ii. Section 17 of the Evidence Act dealing with the definition of admission now includes a statement contained in electronic form as well.  

   iii. Sections 34 and 35 have been amended to include documents maintained in electronic form and electronic record respectively.

   iv. Section 39 dealing with the evidence to be given when statement from a part of a conversation, document, books or series of letters or

198 S. 17 of the Indian Evidence Act: An admission is a statement. Oral or documentary or contained in electronic form, which suggests any inferences as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned.

199 S. 34 of the Indian Evidence Act: Entries in books of account when relevant.

papers has been appropriately amended to include within its gamut ‘electronic records’.

v. Section 59 states that ‘all facts except the contents of document may be provided by oral evidence’. The amendment now permits proving of all facts by oral evidence except contents of document or electronic records. Therefore, one cannot by oral evidence prove the contents of an electronic record.

vi. Section 131\textsuperscript{201} has been amended to include any person in possession of an electronic record. The purpose of the amendment seems to basically inculcate the concept of evidence through electronic records.

b. **Expert opinion on digital signatures:** Section 47A\textsuperscript{202} has been inserted whereby the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact\textsuperscript{203} when the court has to form an opinion as to the digital signature of any person.

c. **Amendments relating to evidentiary value and evidence:** Certain amendments by way of insertions have been made by the IT Act in the Evidence Act to introduce electronic evidence in the Indian legal system. Such electronic evidence has been permitted by use of electronic records before a Court of law. Section 3 was amended to include electronic records within the definition of evidence. In continuation to this amendment, certain further amendments have been made permitting electronic records to be evidence. As to what should be the rules to test the acceptability and genuineness of such electronic records as evidence has been introduced by these amendments. Section 22 A relates to the

\textsuperscript{201} S. 131 of the Evidence Act: Production of document or electronic records which another person, having possession, could refuse to produce.

\textsuperscript{202} Inserted by Information Technology Act, 2000 (w.e.f. 17-10-2000).

\textsuperscript{203} This has an important bearing keeping in mind S. 5 of the Evidence Act which states that, ‘Evidence may be given in any suit or proceeding of the existence or non-existence of every fact in issue and of such other facts are hereinafter declared to be relevant, and of no others.’
relevancy of oral admissions as to the contents of an electronic record produced is in question. Sections 65A\(^{204}\) and 65 B\(^{205}\) collectively from the base for proving the contents of an electronic record. Section 67A deals with proof as to digital signature and 73A relates to proving and verification of digital signature.

d. **Presumption:** Introduction of evidence through electronic records has also led to certain additional presumptions under the Evidence Act. Section 81A provides for presumption of genuineness of Gazette in electronic form. Certain presumptions have been provided for under sections 85A,\(^{206}\) 85B\(^{207}\) and 85C\(^{208}\) relating to electronic agreements, electronic records and digital signatures, and digital signature certificates. Section 88A relates to presumption as to electronic messages and section 90A with regard to presumption as to electronic records which are purported or proved to be five years old.

**Amendment of the Indian Evidence Act, 1872 in ITAA, 2008:** There are also some important amendments in Indian Evidence Act, 1872 by the Information Technology (Amendment) Act, 2008.

e. **Amendment of section 3:** In section 3 relating to interpretation clause, in the paragraph appearing in the end, for the words “digital signature” and “Digital Signature Certificate”, the words “electronic signature” and “Electronic Signature Certificate” shall respectively be substituted.

\(^{204}\) S. 65 A of the Evidence Act deals with special provisions as to evidence relating to electronic record.

\(^{205}\) S. 65B of the Evidence Act deals with admissibility of electronic records.

\(^{206}\) S. 85A of the Evidence Act: Presumptions as to electronic agreements.

\(^{207}\) S. 85B of the Evidence Act: Presumptions as to electronic records and digital signatures.

\(^{208}\) S. 85C of the Evidence Act: Presumptions as to Digital Signature Certificate.
f. **Insertion of new section 45A**: According to section 45A\(^{209}\), when in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact.

   Explanation: For the purpose of this section, an Examiner of Electronic Evidence shall be an expert.

g. **Amendment of section 47A**: In section 47A,
   
   a. for the words “digital signature”, the words “electronic signature” shall be substituted;
   
   b. for the words “Digital Signature Certificate” the words “Electronic Signature Certificate” shall be substituted.

h. **Amendment of section 67A**: In section 67A, for the words “digital signature” wherever they occur the words “electronic signature” shall be substituted.

Amendment of section 85A: In section 85A, for the words “digital signature” at both the places where they occur the words “electronic signature” shall be substituted.

i. **Amendment of section 85B**: In section 85B, for the words “digital signature” wherever they occur the words “electronic signature” shall be substituted;

j. **Amendment of section 85C**: In section 85C, for the words “Digital Signature Certificate” the words “Electronic Signature Certificate” shall be substituted;

---

\(^{209}\) Section 45A deals with opinion of Examiner of Electronic Evidence.
k. Amendment of section 90A: In section 90A, for the words “digital signature” at both the places where they occur the words “electronic signature” shall be substituted;

3. Amendments to Bankers’ Books Evidence Act, 1891:

The Banker’s Books evidence Act, 1891 lays down the rules of evidence in relation to records maintained by banks. Such records are usually needed in cases involving financial and banking transactions, example frauds, cheating cases, financial scams, bouncing of cheques, etc. Section 93 of the Information Technology Act, 2000 amends certain provisions of the Bankers’ Books Evidence Act so as to cover the electronic records maintained by banks.

These amendments have been made as follows:

1. In section 2 –
   
   (a) for clause (3), the following clause shall be substituted namely:

   (3) “bankers books” include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;

   (b) for clause (8), the following clause shall be substituted, namely:

   (8) “certified copy” means when the books of a bank, -

   (a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where
the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank’s business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consists of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.

2. After section 2, the following section shall be inserted, namely:

“Section 2A: Conditions in the printout: A printout of entry or a copy of printout shall be accompanied\(^{210}\) by the following, namely:

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and particulars of-

A. the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

B. the safeguards adopted to prevent and detect unauthorized change of data;

C. the safeguard available to retrieve data that is lost due to systematic failure or any other reasons;

\(^{210}\) Referred to in sub-section (8) of section 2 of Bankers’ Books Evidence act, 1891.
D. the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

E. the mode of verification in order to ensure that data has been accurately transferred to such removable media;

F. the mode if identification of such data storage devices;

G. the arrangement for the storage and custody of such storage devices;

H. the safeguards to prevent and detect any tempering with the system; and

I. any other factor which will vouch for the integrity and accuracy of the system.

(c.) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and behalf, such computer system operated properly at the material time, he was provided with all the relevant data and printout in question represents correctly, or is appropriately derived from, the relevant data”.

4. **Amendments to the Reserve Bank of India Act, 1934:**

   Section 94 of the Information Technology Act, 2000 amended certain provision of the RBI Act, 1934. The only amendment\(^\text{211}\) made has been for giving the Central Board the power to frame regulation for fund transfer through electronic means between the banks or between the bank and other financial institutions shall participate in such fund transfers.

   According to clause “(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other

---

\(^{211}\) By inserting clause (pp) in sub-section (2) of section 58 of RBI Act, 1934.
financial institutions referred to in clause (c) of section 45-I, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the right and obligations of the participants in such fund transfers”.

Critical Appraisal of the Information Technology Act, 2000

The IT Act, 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialized field. The Act has however during its applications has proved to be inadequate to a certain extent. The IT Act, 2000 can be criticized on various counts as under:

The hurry with which the legislation was passed without sufficient public debate, did not really serve the desired purpose. Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for a public debate. The IT Act, 2000 in their very preamble and aim state that they are targeted at aiding e-commerce and are not meant to regulate cyber crime”, which is also one of the inadequacy to deal with cases of cyber crime.

a. Cyber torts: the recent cases including the cyber stalking, cyber harassment, cyber nuisance have shown that the IT Act, 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which need to be taken care of.

b. Cyber crime in the Act is neither comprehensive nor exhaustive: There is need of dedicated legislation on cyber crime that can supplement the IPC. The IT Act, 2000 is not comprehensive and doesn’t even define the term cyber offences. “India as a nation has to cope with an urgent need to regulate and punish those committing cyber crimes, but with no specific
provisions to do so. Supporters of the IPC School vehemently argue that IPC has stood the test of time and that it is not necessarily to incorporate any special laws on cyber crimes. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms the argument does not have appropriate backing. It has to be distinctively understood that cybercrime and cyberspace are completely new whelms, where new possibilities and opportunities emerge by the day in the form of new kinds of crimes.

c. Ambiguity in the definition: The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication and wrong interpretation. There is every possibility of this section being misapplied and wrongly interpreted by the subordinate judiciary, therefore, the need is to give the precise definition.

Further section 67 is also vague to certain extent. It is difficult to define the term lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by the Bal Bharti School Case.

d. Uniform Law: The need of the hour is worldwide uniform cyber law to combat cyber crimes. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level, e.g., the author of the love bug virus was appreciated by his countrymen.

e. Lack of awareness: One important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the public about there rights. Further most of the cases are going unreported if the people are vigilant about their rights and the law definitely protect their rights. E.g. the Delhi high court in October 2002 prevented a person from selling the Microsoft Pirated Software over an auction site. Achievement was also made in the case before the court of MM Delhi wherein a person
was convicted for online cheating by buying Sony products using a stolen creditcards.

f. Jurisdictional issue: Jurisdiction is also one of the debatable issues in the cases of cyber crimes due to the very universal nature of cyber crime. With the ever – growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to conventional methods. The Act of 2000 is very silent on these issues.

g. Extra-territorial jurisdiction: Though section 75 provides for the extra territorial operations of this law, but they could be meaningful only when backed with the provisions recognizing orders and warrants for information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

h. Raising the Cyber army: Cybercrime is a high-tech crime committed by the persons who are highly qualified in the computer software technology, therefore, the prevention, investigation and enforcement of this unique category of crime requires a police force well trained in handling the software technology. The government has taken a step in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the cyber crime investigation cell (CCIC) of the CBI is definitely a welcome step in this direction. The IT Act of 2000 is silent on this aspect.

i. Cyber Savvy Bench: Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the PIL, which the Kerela High Court has accepted through an e-mail.
j. Dynamic form of cyber crime: Speaking on the dynamic nature of cyber crime FBI director Louis Freeh has said: “In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind”. The de-creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.

k. Hesitation to report offences: One of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the Delhi time theft case. “The police are a powerful force today which can play an instrumental role in preventing cyber crimes. At the same time, it can also end up wielding the rod and harassing innocents, preventing them from going about their normal cyber business”. For complete realization of the provisions of this Act a cooperative police is require.

D. Information Technology (Amendment) Act, 2008

With the passage of time and advancement in technology new methods of committing crime using Internet and computer surfaced, the need was felt to amend the IT Act, 2000. New forms of cybercrimes had appeared on Indian scene posing a challenge before the law makers who were faced with two hard options, namely, either to drastically amend the existing law to give it some teeth or to helplessly see it openly outraged and violated by the cyber criminals and others.

At this critical juncture was brought the draft of the Information Technology Amendment Bill, 2006 which was introduced on December 15, 2006 in the Lower House of Parliament. It was scrutinized by an Expert Committee which suggested several changes. The gravity of the issue of emerging cyber crimes on national and global scales had worried
the lawmakers so much that they refer it to the Standing Committee of Parliament to finally suggest changes necessary to make the enactment more effective and in agreement with India’s international obligations as an IT power.

It took a couple of years before the amendments could see the light of the day. The Information Technology (Amendment) Bill, 2006 was further amended by the Information Technology (Amendment) Bill, 2008; and in the process, the underlying Act was renamed as the Information Technology (Amendment) Act, 2008. The Information Technology Amendment Act, 2008 was passed by the Lower House on December 22’ 2008; and by the Upper House on the following day i.e. December 23, 2008.

Later the government has come out with the Cyber Appellate Tribunal (Salary, Allowances and other Term and Condition of service of Chairperson and Members Rules), 2009; the Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour in Capacity of Chairperson and Members) Rules, 2009; the Information Technology (Procedure and safeguards for Interception, Monitoring and Decryption of information) rules, 2009; the Information technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009; and Information Technology (Procedure and Safeguard for Monitoring and Collecting traffic Data or Information) Rules, 2009.

The latest rules notified by the government in the year 2011 include; the Information Technology (Electronic Service Delivery) Rules, 2011; the Information technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011; the Information technology (Guidelines for Cyber Café) Rules, 2011.
The Information Technology (Amendment) Act, 2008\textsuperscript{212} has introduced remarkable changes in the IT Act, 2000 on several counts, which deserve to be discussed exhaustively as under:

(1) **Electronic Signatures introduced**

With the passage of the IT (amendment) Act, 2008 India has become technologically neutral due to adoption of electronic signature as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures. This is a positive change as India has different segments people and all may be not technologically adept to understand and use the digital signatures. Therefore, allowing forms of authentication that are simpler to use such as retina scanning can be quite useful in effective implementation of the Act. Further, in a move to secure the flow of data and information on the internet, and promote e-commerce & e-governance, the amended act in Section 84 A has empowered the Central Government to prescribe modes or methods for encryption. These parameters should be laid down in consultation with organizations such as Nasscom and/ or governmental agencies that can assist in formulation of necessary standards and related rules.

(2) **Corporate responsibility introduced\textsuperscript{213}**

The corporate responsibility for data protection is incorporated in S 43 A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of ‘reasonable security practices’ to maintain its secrecy, failing which they may be liable to pay damages. Also, there is

\textsuperscript{212} Information Technology (Amendment) Act, 2008 w.e.f. 27-10-2009.

\textsuperscript{213} Section 43 A.
no limit to the amount of compensation that may be awarded by virtue of this section. This section must be read with Section 85 of the IT Act, 2000 whereby all persons responsible to the company for conduct of its business shall be held guilty incase offence was committed by a company unless no knowledge or diligence to prevent the contravention is proved.

(3) **Important definitions added**-

Two very important definitions are added to the It Act through IT Amendment Act, 2008- “Communication device”\(^{214}\) and “intermediary”\(^{215}\). Although cell phones and other devices used to communicate would fall under the definition of the computer in the IT Act. This amendment remove any ambiguity and brings within the ambit of the Act all communication devices, cellphones, iPods or other devices used to communicate, send or transmit any text, video, audio or image. The insertion of definition of “intermediary” similarly clarifies the categories of service provider that come within its definition that includes telecom service providers, network service providers, internet service provider, webhosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

(4) **Legal validity of electronic documents re-emphasized**-

Two new Sections\(^{216}\) in the amended Act reinforce the equivalence of paper based documents to electronic documents. Section 7A in the amended Act makes audit of electronic documents also necessary where paper based document are required to be audited by law. Section 10A confers legal validity & enforceability on contracts formed through electronic means. These provisions are inserted to clarify and strengthen the legal principle in Section 4 of the IT Act, 2000 that electronic

\(^{214}\) Section 2 (ha)

\(^{215}\) Section 2 (w)

\(^{216}\) Section 7A and Section 10A.
documents are at par with electronic documents and e-contracts are legal recognized and acceptable in law. This will facilitate growth of e-commerce activity on the internet and build netizen’s confidence.

(5) **Power of Controller under the amended Act**

The role of the Controller to act as repository of digital signatures has been repealed by the IT Amendment Act, 2008. This role has been assigned to the Certifying Authority in Section 30 of the IT Act. This change poses a major challenges to ensuring the secrecy and privacy of electronic signature is maintained. The Certifying authorities will bear greater responsibility and need to strengthen their security infrastructure to ensure its role as repository is delivered with efficacy. It will need to allocate more resources and manpower to regularly publish information regarding its practices, electronic signatures certificates and publish the current status of each certificate.

(6) **The Role of Adjudicating officers under the amended Act**

The Adjudicating officer’s power under the amended Act in Section 46 (1A) is limited to decided claims where claim for injury or damage does not exceed 5 crores. Beyond 5 crore the jurisdiction shall now vest with competent court. This has introduced another forum for adjudication of cyber contraventions. The words “competent court” also needs to be clearly defined. As per Section 46(2), the quantum of compensation that may be awarded is left to the discretion of Adjudicating officers. These leaves a wide room for subjectivity and quantum should be decided as far as possible objectively keeping in view the parameters of amount of unfair advantage gained amount of loss caused to a person (wherever quantifiable), and repetitive nature of default. The Information Technology (qualification and experience of adjudicating officers and
manner of holding enquiry) Rules, 2003 lay down the scope and manner of holding inquiry including reliance on documentary and other evidence gathered in investigation. The rules also provide for compounding of contraventions and describe factors that determine quantum of compensation or penalty.

In the IT Act, 2000 the office of adjudicating officer had the powers of civil court and all proceedings before it are deemed to be judicial proceedings. A new change is incorporated in Section 46 (5) © whereby the Adjudicating officers have been conferred with powers of execution of orders passed by it, including order of attachment and sale of property, arrest and detention of accused and appointment of receiver. This empowers the office of Adjudicating officer and extends greater enforceability and effectiveness of its orders.

(7) Composition of CAT-

The amended Act has changed the composition of the Cyber Appellate Tribunal. The Presiding officer alone would earlier constitute the Cyber Regulation Appellate Tribunal which provision has been now amended. The tribunal would now consist of Chairperson and such numbers of members as Central Government may appoint. The qualifications for their appointment, term of office salary, power of superintendence, resignation and removal, filling of vacancies have been incorporated. The decision making process allows more objectivity with Section 52 D that provides that the decision shall be taken by majority.

It is pertinent to note that there has not been any amendment in Section 55 by 2008 amendments which states that no order of CAT shall be changed on ground that there existed a defect in constitution of appellate tribunal. However in many views this runs contrary to principles of natural justice. An analogy is drawn to Arbitration where defect in
constitution of a tribunal renders an award subject to challenge as per Indian laws.

(8) **New Cybercrimes as offence under amendment Act**-

Many cybercrimes for which no express provisions existed in the IT Act, 2000 now stand included by the IT (Amendment) Act, 2008 such as sending of offensive or false messages, receiving stolen computer resource, identity theft, cheating by personation, violation of privacy. A new offence of Cyber terrorism is added which prescribes punishment that may extend to imprisonment for life. For other offences punishment prescribed is generally up to three years and fine of one/two lakhs has been prescribed and these offences are cognizable and bailable. This will not prove to play a deterrent factor for cyber criminals. Further, as per new S. 84 B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new S. 84C makes attempt to commit an offence also a punishable offence with imprisonment for a term which may extend to one half of the longest term of imprisonment provided for that offence.

In certain offences, such as hacking, punishment is enhanced from 3 years of imprisonment and fine of 2 lakhs to fine of 5 lakhs. In S. 67, for publishing of obscene information imprisonment term has been reduced from five years to three years (and five years for subsequent officer instead of earlier ten years) and fine has been increased from one lakh to five lakhs (ruppes ten lakhs on subsequent conviction). Section

---

217 S. 66A  
218 S. 66B  
219 S. 66C  
220 S. 66D  
221 S. 66E  
222 S. 66F  
223 Mentioned in Section 66  
224 S. 66
67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that may extends to 5 years with fine upto ten lakhs.\footnote{This provision was essential to curb MMS attacks and Video vouyerism.} Section 67B punishes of child pornography, child’s sexually explicit act or conduct with imprisonment on first conviction for a term upto 5 years and fine upto 10 lakhs. This is a positive change as it makes even browsing and collecting of child pornography a punishable offence.

Punishment for disclosure of information in breach of lawful contract under sec. 72 is increased from 2 yrs upto 5 yrs and from one lakh to five lakh or both. This will deter the commission of such crime. By virtue of Section 84B person who abets a cybercrime will be punished with punishment provided for that offence under the Act. This provision will play a deterrent role and prevent commission of conspiracy linked cybercrime. Also, punishment for attempt to commit offences is given under Section 84C which will be punishable with one half of the term of imprisonment prescribed for that offence or such fine as provided or both.

(9) Section 67 to play a significant role in cyber crime prosecution-

Section 67 brings a very significant change in the IT Act, 2000. According to this section, intermediaries shall be bound to preserve and retain such information as may be prescribed by the Central Government and for such duration and format as it may prescribe. Any intermediary that contravenes this provision intentionally or knowingly shall be liable on conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lakh or both. Many cybercrime cases cannot be solved due to lack of evidence and in many cases this is due to the fact that ISP failed to preserve the record pertaining to relevant time. This provision is very
helpful in collection of evidence that can provide indispensable in cybercrime cases.

(10) **Power of the Controller to intercept amended** \(^{226}\) 

Section 69 deals with power of Controller of intercept information being transmitted through a computer resource when necessary in national interest is amended by Section 69. In fact the power vests now with the Central Government or State Government that empowers it to appoint for reason in writing, any agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The procedure and safeguards to exercise this power are laid down out by the Information Technology (procedure and safeguard for interception, monitoring ad decryption of Information) Rules, 2009.

The subscriber or intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 7 yrs and imposition of fine. The element of fine did not exist in the erstwhile Section 69. The said rules provide ample safeguards to ensure the power in this section is diligently exercised, with due authorization procedure compiled with and not abused by any agency/ intermediary including maintaining confidentiality and rules for maintaining or destruction of such records.

(11) **Power to block unlawful websites should be exercised with caution** \(^{227}\) 

Section 69A has been inserted in the IT Act by the amendments in 2008 and gives power to Central Government or any authorized officer to direct any agency or intermediary (for reason recorded in writing) to block websites in special circumstances as applicable in Section 69. Under this

---

226 Section 69.
227 Section 69A.
Section the grounds on which such blocking is possible are quite wide. In this respect, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 were passed vide GSR 781 (E) dated 27 October 2009 whereby websites promoting hate content, slander defamation, promoting gambling, racism, violence and terrorism, pornography, violent sex can reasonably be blocked. The rules also allow the blocking of websites by a court order.

(12) **Confirmation of Power to collect, monitor traffic data**

As a result of the amendments in 2008, Section 69 B confers on the Central Government power to appoint any agency to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource in order to enhance its cyber security and for identification, analysis, and prevention of intrusion or spread of computer contaminant in country. The Information Technology (procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009 have been laid down to monitor and collect the traffic data or information for cyber security purpose under Section 69B. It places responsibility to maintain confidentiality on intermediaries, provides for prohibition of monitoring or collection of data without authorization. It also provides for review of its decision and destruction of records.

(13) **Significance of the term “Critical Information Infrastructure”**

Section 70 has a very important definition added by the IT (Amendment) Act, 2008. The explanation to Section 70 defines what “critical information infrastructure” is. It encompasses the computer resource the destruction of which not only has an adverse impact on

---

228 Section 69B.
229 Section 70.
defence of India but also economy, public health or safety. This is very significant step as today our IT infrastructure may also be used to manage certain services offered to public at large, destruction of which may directly affect public health and safety. Hence, their protection is equally important as it is maintaining of security and sovereignty of India.

Indian CERT has been appointed as the National Nodal Agency for critical information infrastructure protection. The CERT plays an indispensable role in maintaining cyber security within the country. A very important step is coordination between CERT and service providers, data centres, body corporate and other persons. That will lead to effective performance of the role of CERT in. It also excludes the court from taking cognizance of any offence under this section except on a complaint mad by authorized officer of CERT to prevent misuse of the Section.

(14) Important clarifications on the Act’s application & effect-

By virtue of Section 77 in the amended Act, it has been defined that awarding of compensation, penalty imposed or confiscation made under this Act shall not prevent the award of compensation or imposition of any other penalty or punishment under any law for the time being in force. This Section can be read with Section 81 proviso wherein it is clarified that IT Act shall not restrict any person from exercising any right conferred under copyright Act, 1957 or patents Act, 1970.

(15) The combined Effect of Sections 77 and 77B-

Compounding of offences other than offences for which imprisonment for life or punishment for a term exceeding has been
provided has been possible. Section 77B makes offences punishable with imprisonment of three years and above as cognizable and offence punishable with 3 years of punishment as bailable.

(16) **Combined Effect of Sections 78 & 80**

The Section 78 of the Act is amended to confer power to investigate offences under the Act from DSP level to Inspector level. This will be instrumental in quicker investigation in the cybercrime cases provide adequate tools and training is provided. Section 80 has amended and power to enter and search in a public place is now vested in any police officer not below the rank of the inspector or any authorized officer of central government or state government.

(17) **Liability of Intermediary amended**

The amended Section 79 states that the intermediary shall not be liable for any third party information if it is only providing the access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted or the intermediary does not initiate the transmission, select the receiver and select or modify the information contained in transmission. It provides that the Intermediary shall be liable if he has conspired or abetted or induced, whether by threats or promise or otherwise in the commission of the unlawful act.\(^{232}\) However, it is pertinent to note that the onus to prove conspiracy has now shifted on the complaint. This may be extremely difficult for a complainant to prove.

Section 3(b) renders an intermediary liable in case upon receiving actual knowledge or on receiving notice from a government agency, the

\(^{232}\) Section 79(3)(a).
intermediary fails to expeditiously remove or disable access to the unlawful material without vitiating the evidence in manner.

(18) **Examiner of Electronic Evidence created**

With amendment in 2008, Section 79 A is added that empowers the Central Government to appoint any department or agency of Central or State Government as examiner of Electronic Evidence. The explanation to the Section has an inclusive definition of “electronic from evidence” that means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cellphones, and digital fax machines. With the increasing number of cybercrime cases it will become necessary to set up at least one examiner of Electronic Evidence in each State. The CFSIL laboratory in Hyderabad is playing similar role at present in cybercrime cases where forensic study of hard discs and other computer accessories, digital equipment is undertaken to provide expert opinion on the digital evidence analysed.

E. **Efficacy of the Existing Cyber Law**

The IT Act, 2000 was amended by the IT (Amendment) Act, 2008. The object of the Amendment Act was to strengthen the existing legislation to curb the cybercrime by abrogating the infirmities of the IT Act and to make it a suitable legislation for combating the cybercrime effectively. However, it is apposite to state that the Amendment Act could not address the legislative weaknesses of the law. This segment deals exclusively with the infirmities and shortcomings which the Amended Act is suffering from and to ascertain as to how the existing cyber law can be strengthened to make it efficacious and effective to counter the escalating menace of cyber crimes being committed against the individuals, institutions, society at writ large and the governments.
Non-coverage of many crimes:

While there are many legislations not only in many Western countries but also some smaller nations in the East, India has only one legislation—the I T Act, 2000.233 The IT Act, 2000, though a landmark legislation to deal with the cybercrime in India but the Act could not provide exhaustive measures to counter the rising trend in the cybercrime, for despite the amendment incorporated in it to attune it with the need to curb the cybercrime in view of the technological development in the area of information technology, a number of crimes and important issues have been left unaddressed. Many of the cyber crimes like cyber squatting with an evil attention to extort money, Spam mails, ISP’s liability in copyright infringement, data privacy issues have not been given adequate coverage in the legislative scheme of the Act. In order to make the Act efficacious and effective following measures need to be addressed:

1. The Amendment Act of 2008 has failed to define word “Hacking” or “Hacker”, surprisingly the act of hacking with the very word “hacking” finds a mention in section 66 of the original Act.

2. The new amendments under Section 43-A make it mandatory for corporate “possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices”.

3. The IT Rules, 2011 framed under the Sec 43-A having sub section 8(2),8(3) and 8(4) which relates to the introduction of ISO 27001 as a mandatory compliance requirement through the backdoor with the use of misleading words mentioned in the rules. ISO 27001

Compliances and Audit now has additional compliance obligation for organizations.

4. Section 79 of the amended IT Act, 2000 is not a penal section under the Act. Penalty under the Act would arise on any person or a body corporate. When an incident has occurred on account of other sections such as Sec. 43, 43-A, 65, 66, 66A, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 69, 69A, 69B, 70, 71, 72, 72A, 73, 74, 84B, 84C etc. which can be brought under any of these sections and the person who is accused is otherwise an “Intermediary” as defined under the Act, then the provisions of Section 79 apply. These provisions give him an opportunity to escape his liability. To use these provisions he needs to act such in a manner which can be considered as “exercising Due Diligence”. The privileged intermediaries include telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

5. The amended IT Act, 2000 has not specifically dealt with the issue pertaining to e-discovery. Today, organizations are relying increasingly upon digital evidence like email etc. and media as a means of communicating with each other and conducting business. IT Act, 2000 remains silent on this issue and also leave scope for business exploitation of e-discovery by large consulting firms at their own interpretation.

6. The IT Act, 2000 have not dealt with spam issue in a comprehensive manner. The definitions section does not define the word spam nor is even mentioned anywhere in the Act. The practice of sending unsolicited emails is getting rampant in India which also amounts to
breach of individuals right to privacy on the net. While India already features on the top ten nations from where spam originates. The legislature did not think of taking exclusive cognizance to this huge menace, which jams our new national resource “the bandwidth”.

7. A Cyber Café is also a “Intermediary” hence the obligations under Section 79 and the rules framed there in for “Intermediaries” already apply to Cyber Cafes. The rules for Cyber Cafes are incomplete rules requiring further rules making at the State Government level. The rules also infringe on the power of the State Government for maintaining law and order in the State.

8. Cyber Squatting which relates to stealing or assuming a domain name of a established brand by a new or less known brand or a comp Act.

9. The crime of pornography by foreign websites is let loose and is not discussed nor being penalized. This flaw also make Indian cyber criminal to host their pornography related website’s on foreign shores without being accounted for in Indian territory.

10. Taxation of ecommerce transactions when a transaction is committed from Indian jurisdiction is not explicitly discussed nor is any passing reference made with a view to bind it with Indian tax law.

11. Cyber crime committed by websites of foreign origin like spreading of viruses and worms, selling banned medicines and drugs, selling devices harmful for India internal security etc do not find a mention in the IT Act, 2000.

12. Jurisdiction of electronic contracts is not clearly defined in the Act. Cross border contracts since “Click-Wrap” contracts are not legally recognized as equivalent to digitally signed contract, body corporate
relying on “Click-Wrap Contracts” (Where the user clicks on a button or checkbox I agree”) need to take such additional measures as may be required to provide a supplementary evidentiary base for validating the contracts.

13. A clear section with regards to Jurisdiction of courts over parties staying or operating in different jurisdictions or countries is not covered. Even though having a complete separate legal jurisdiction for the cyber world, is not an expectation but certain clear guidelines necessary help lower courts and humble netizens.

14. Law remains silent for stamp duty on electronic contracts. eStamp duty if permitted can yield lot of revenue to the government.

15. Internet hours theft being completely intangible and different type of theft other then theft of tangible items. Internet hours of bandwidth theft are not taken care of in the IT Act, 2000. Resource to section 379 of the IPC may not result in justice for reason of interpretation.

16. There is no power given to police for entering and searching private places. Many cyber criminal operates from homes where police cannot search. Also major penal sections though cognizable are also bailable, this option allows the accessed to seek and get anticipatory bail before even action begins.

17. Major offences covered under this Act are bailable. Thus interim reliefs, anticipatory bails etc. would be in a vogue with cyber criminals.

18. The IT Act, 2000 does not explicitly consider Intellectual Property Rights in the Internet domain.

19. The phraseology of Section 66A is too vague and tantamount to abuse. The provision is violative of Articles 14, 19(1)(a) of the
Constitution of India.\textsuperscript{234} Section 66A is breach of fundamental rights. It is absolutely draconian as it gives the authorities an occasion to misuse and deprive citizens of their personal liberty. If section 66A is allowed to be continued in the Act, it will foreclose debates and discussion which is inherently essential for the democracy to survive. Its chilling effect is already visible—the jailing of a professor in Kolkata, a businessman in Tamil Nadu and two young women in Mumbai, for casual cyber writings, or simply forwarding of received material. Today, netizens are victims, but next journalists will be threatened, as most of their writings are uploaded to the Net, too. This is a potential tool in the hands of rulers to curtail the voice of opposition. It is fatal for the freedom of speech of netizens in general and the press in particular. The executive should delete it from the IT Act or refrain from using it.\textsuperscript{235}

**STATISTICAL REALITIES OF CYBER CRIME IN INDIA**

The efficacy of the cyber law regime in India can be assessed in the light of the ground realities that emerge from the study of the statistics of the cybercrime cases and the increasing trends revealed by the statistics as under:

\textsuperscript{234} KRISHNA MOHAN VENIGALLA: THE HINDU, Posted on: May 17, 2013 at 10:22 IST.
# Cyber crimes/cases registered and persons arrested under IT Act during 2009-2012

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Crime Heads</th>
<th>Cases registered</th>
<th>Percentage Variation in 2012 over 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2009</td>
<td>2010</td>
</tr>
<tr>
<td>1.</td>
<td>Tampering computer source documents</td>
<td>21</td>
<td>64</td>
</tr>
<tr>
<td>2.</td>
<td>Hacking with computer system i)Loss to computer utility ii)Hacking</td>
<td>115</td>
<td>346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>118</td>
<td>164</td>
</tr>
<tr>
<td>3.</td>
<td>Obscene Publication in electronic form</td>
<td>139</td>
<td>328</td>
</tr>
<tr>
<td>4.</td>
<td>Failure in complying orders of Certifying Authority</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>5.</td>
<td>Unauthorized access to protected systems</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>Fraudulent obtaining of licence or digital signatures</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>7.</td>
<td>Publishing false digital signature certificate</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>8.</td>
<td>Fraud digital signature certificate</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>9.</td>
<td>Breach of Confidentiality/ Privacy</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>10.</td>
<td>Other</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td><strong>420</strong></td>
<td><strong>966</strong></td>
</tr>
</tbody>
</table>

Source: Cybercrimes in India-Compendium-2012-National Crime Record Bureau.
A total of 2,876 cases were registered under the IT Act, 2000 during the year 2012 as compared to 1791 cases during the previous year 2011, thereby reporting an increase of 60.6% in 2012 over 2011. 16.4% cases (471 out of 2,876 cases) were reported from Maharashtra followed by Andhra Pradesh (429), Karnataka (412), Kerala (269) and Uttar Pradesh (205).

50.1% (1440 cases) of the total 2876 cases registered under IT Act, 2000 were related to loss and damage to computer resource/utility registered under hacking with computer systems. 612 persons were arrested for committing such offences. There were 589 cases of obscene publication or transmission in electronic form during the year 2012, wherein 497 persons were arrested. Out of the total (1875) hacking cases, the cases relating to loss or damage of computer resource utility under Section 66 (1) of the IT Act were 76.8% (1440 cases) whereas the cases relating to hacking under Section 66(2) of the IT Act were 23.2% (435 cases).
Cyber Crimes registered under Indian Penal Code during 2009-2012

Source: Cybercrimes Compendium-2012: NCRB.

<table>
<thead>
<tr>
<th>Sl. No</th>
<th>Crime Heads</th>
<th>Cases registered</th>
<th>% Variation in 2012 over 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2009</td>
<td>2010</td>
</tr>
<tr>
<td>1.</td>
<td>Offences by/against public servants</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>2.</td>
<td>False electronic evidence</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>Destruction of electronic evidence</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4.</td>
<td>Forgery</td>
<td>158</td>
<td>188</td>
</tr>
<tr>
<td>5.</td>
<td>Counterfeiting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Property Mark</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ii) Tampering</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>iii) Currency/Stamps</td>
<td>21</td>
<td>7</td>
</tr>
<tr>
<td>6.</td>
<td>Criminal Breach of Trust</td>
<td>90</td>
<td>146</td>
</tr>
<tr>
<td>7.</td>
<td>Total</td>
<td>276</td>
<td>356</td>
</tr>
</tbody>
</table>

A total of 601 cases were registered under IPC Sections during the year 2012 as compared to 422 such cases during 2011, thereby reporting an increase of 42.4 percent. Majority of crimes out of total 601 cases registered under IPC fall under two categories viz. criminal breach of trust or fraud (282) and forgery (259). Although such cases fall under the traditional IPC crimes, these cases have the cyber overtones wherein computer, internet or its enabled services were present in the crime and hence they were categorized as cyber crimes under IPC. Cyber forgery (259 cases) accounted for 0.27% out of the 94,203 cases reported under
cheating. Cyber frauds (118) accounted for 0.66% of the total criminal breach of trust cases under IPC (17,201).

The Cyber crimes are on the rise but very few police complaints are made and even fewer of these become FIRs. Instances of the accused being prosecuted are rare. As a result, cyber crime convictions in India in the past 10 years number less than ten and have no correlation to contemporary reality, says cyber law expert and advocate Pavan Duggal. According to a survey done by him, for every 500 cyber crimes, only 50 get reported to the police, and just one out of this 50 is registered as an FIR.

The Information Technology Act, 2000, was enacted primarily to provide a platform for e-commerce to take off in India. Only certain types of cyber crimes like hacking, malicious change to source code, breach of protected systems and publishing false digital certificates were dealt with in the Act. As a result, the police invariably relied on the Indian Penal Code to register cases involving cyber crime. The IT Act was a new creature to them and most of the cases continued to be registered under the Indian Penal Code sections 420 (cheating), 406 (criminal breach of trust) and the forgery sections. The amendments to the Act in 2008 brought new cyber crimes within its ambit like cyber stalking, cyber defamation, cyber nuisance, cyber harassment, identity theft, breach of privacy and cyber terrorism.

But these amendments have not produces the desired effect. The amendments erred fundamentally in that while the law was widened to bring more crimes under its purview, the quantum of punishment for most offences was significantly reduced. Except for major cyber crimes like cyber terrorism, breach of protected systems and child pornography all other offences were made bailable offences. As a result, the conviction rate has gone for a toss. Offences in the original Act punishable with five
years’ imprisonment have been reduced to three years by the amendment. So the deterrence value of the Act has come down.

The efficacy of the Act could have been far more than what it presently is. With the advent of social media, cyber crimes are happening at the drop of a hat.236 There are not enough, or adequately trained, police personnel to handle cyber crimes. There is also a problem of perception as policemen see these as minor crimes. Evidences in such crimes have to be seized quickly due to their electronic nature and ease of deletion. The budgetary constraint is yet another reality that haunts the capacity building to make the law regime more efficacious. The Central Forensic Science Laboratories are overburdened with work. Charge sheets are being filed without the electronic evidence component because of delays - ranging from few months to a year – by the labs to send back forensic report. It is not out of way to predict in view of the escalating cyber crime that by the year 2015, one out of every four cases will have an electronic component and the challenge will be to capture electronic evidence instantly. The IT Act does not sufficiently cover social media crimes and mobile phone crimes. Technology legislation has to keep pace with the fast developments in the area of information technology and computer science.

The implementation of the Information Technology Rules, 2011, is a welcome move as it mandates provisions for Internet Service Providers and other intermediaries to store all transaction information including personal data for a reasonable period of time. This will help trace offenders. To improve deterrence, the Information Technology Act has to be constantly amended to cover more cyber crimes and the quantum of punishment needs to be increased.

***