Chapter-2 "Government Policies & Promotion of IT Industry in India"

2.1 Introduction
2.2 IT Policy of the Government
2.3 E-Governance
2.4 Organisational and Human Resources Development
2.5 Personal Management System
2.6 Delivery of Services
2.7 Cyber Laws
2.8 IT Industry in India
Chapter-2

Government Policies & Promotion of IT Industry In India

2.1 INTRODUCTION

The Government in the ultimate analysis is an information processing entity. All government servants are knowledge workers. Whatever the area of activity every government organisation, is concerned with collecting information or using information to administer the laws, rules & procedures so that the objective of that organisation are achieved.

When it comes to brass tacks, government exist to ensure that the society is able to live peacefully according to the rule of law and there is a systematic effort at economic development. So whether it is regulatory administration or development administration, when the chips are down, ultimately it amounts to intelligent and effective use of Information.

In government systems, the processing of information decides the culture of the organization, everyone complains about the delay in administration. If we go to the bottom of it, we find that the delay is because of the delay in either collecting or collecting or accessing information. The greater the speed with which information can be collected, collected and accessed less will be the time taken.
Another reason for the delay is that the entire govt. operators on the principle that justice must not be done but must seen to be done. So, every case has to be examined in the context of the precedents in the context of precedents adopted and the rules. It means that one has to keep records and also have access the relevant record as quickly as possible. Many a time this is also a factor that causes delay.

Delay in government System, in turn, leads to corruption. Speed money is a very common source of corruption. If we are able to eliminate delays logically, to some extent, the speed money corruption also can be checked. Another source of corruption is the limited access of information.

There are seen examples in Rajasthan that the egos were able to point out how funds are misused in IRDP and other poverty alleviation programmes by. Informing the beneficiaries about the funds allotted to their village providing information become a route for increasing awareness of the people and raising their consciousness Traditionally Governments have guarded the access information rigidity because there is another aspect to information across namely, security. The Official Secrets Act highlights the need for protecting the society and not compromising on the security issue. But this is a Gary area where under the guise of security and national interests a lot of information can be classified as secret. The Right to Information Act has broken the fences now.

Added to this the power dynamics in the government administration. Access to information capacity for recalling the relevant information or controlling information in which a citizen may be interested are factors which give power to the bureaucrat. The bureaucrat who is either drunk on power or is after corruption can use this aspect of information dynamics in government to line his own pocket.
2.2 IT POLICY OF THE GOVERNMENT

The Government has set up clear policy agenda for its own e-governance and for promotion of IT Industry also:

National e-governance Plan

The national e-governance plan (2003-07) reflects the strategic intent of the central government in the right perspective. Many projects are earmarked under this plan, and it is trying to address the digital divide. The plan seeks to create the right governance and institutional mechanisms, set up the core infrastructure and policies and implement a number of Mission Mode Projects at the center, state and integrated service levels to create a citizen-centric and business-centric environment for governance. The Government has attributed the following emphasis on the plan:

- Adequate weightage must be given for quality and speed of implementation in procurement procedures for IT services
- Incorporation of suitable system of incentivization of states to encourage adoption
- Trend of delivery of services through common service centres should be encouraged and promoted
- Wherever possible services should be outsourced
- Full potential for private sector investment should be exploited
- Connectivity should be extended up to block level through NICNET/ SWANs

Minimum agenda for e-governance

The minimum agenda for e-governance in each Ministry has been devised as follows:

(i) (a) Each Ministry/Department must provide PCs with necessary software up to the Section Officer level.

(b) LAN must also be set up.
(ii) (a) 100% training of all staff who have access to and need to use computers for their office work should be ensured.  

(b) For this purpose, inter alia, Ministries/Departments should set up or share Learning Centres for decentralized training in computers as per the guidelines issued by the DIT.

(iii) Each Ministry/Department should start using the Office Procedure Automation software developed by NIC with a view to keeping a record of receipt of dak, issue of letters, as well as movement of files in the department.

(iv) Pay roll accounting and other house-keeping software should be put to use in day-to-day operations.

(v) (a) Notices for internal meeting should be sent by email to the officers;

(b) Similarly, submission of application for leave and for going on tour should also be done electronically;

(c) Ministry/Department should also set up on-line notice board to display orders, circulars etc. as and when issued.

(vi) Ministries/Departments should use the Web-enabled Grievance Redressal Software developed by Department of AR & PG. Each Ministry/Department should have its own website.

(viii) All Acts, Rules, Circulars should be converted into electronic form and, along with other published material of interest or relevance to the public, should be made available on the internet and be accessible from the Information and Facilitation Counter.
(ix) (a) The websites of Ministries/Departments/Organisations should specifically contain a section in which various forms to be used by citizens/customers are available. The forms should be available for being printed out or for being completed on the computer itself and then printed out for submission.

(b) Attempts should also be made to enable completion and submission of forms online.

(x) The Hindi version of the content of the websites should be developed simultaneously, as far as possible.

(xi) Each Ministry/Department would also make efforts to develop packages so as to begin electronic delivery of services to the public.

(xii) Each Ministry/Department should have an overall IT vision or strategy for a five year period, within which it could dovetail specific action plans and targets (including the minimum agenda) to be implemented within one year.

States' IT Policy of Andhra Pradesh

Almost all the states have laid down their policy for the development of Information technology industry in their respective states. According to Sudhir Narang, Vice-president, government & service provider business, Cisco Systems, India & SAARC, "Almost every state has an IT policy in place with the aim of evolving itself from being an IT-aware to an IT-enabled government. State governments are fast recognising the benefits of an IT-enabled working environment." As of now, e-governance projects are being run only in certain departments. This approach will gradually be extended to all departments eventually, leveraging the power of IT to streamline administrative functions and increase transparency.
2.3 E-GOVERNANCE

India could well be on the way to becoming an information and knowledge society and contrary to popular perception, its impact will be far-reaching, down to the villages and could bridge traditional divides. E-Governance is the next step - it promises to provide karmic relief from corrupt officials and politicians.

The Indian government is using IT to facilitate governance. The IT industry is doing its bit to help, as public-private partnerships become the order of the day. Information technology is going to be the decisive technology in the years to come. It is a combination of computers and communication. The characteristic of information technology are such that if it is intelligently and imaginatively used, many if the negative aspects of the dynamics of information processing and information handling in Government can be overcome IT in short can be used as a tool for a more responsive and effective administration.

After all IT has features which when we come to think of it, appear as if they have been designed for handling a system like a government:

i. IT brings enormous speed in processing of information.

ii. Random access memory is characteristic of information technology and this is another important aspect of govt. administration.

iii. Diffusion of information can be done on a much wider basis and much more effectively that what is possible in the past. Everyone today is talking about the internet. After all, with 70 million people accessing a whole lot of databases is classic example of the enormous diffusion power of IT.

iv. The IT can eliminate many middle level posts in management. Hierarchy is one of the factors that causes delay in the movement of papers and the processing.. Information in government and information technology can eliminate the element of delay by hierarchy. It can empower the public access to information can becomes easier.
The last couple of years have seen e-governance drop roots in India. IT enables the delivery of government services as it caters to a large base of people across different segments and geographical locations. The effective use of IT services in government administration can greatly enhance existing efficiencies, drive down communication costs, and increase transparency in the functioning of various departments. It also gives citizens easy access to tangible benefits, be it through simple applications such as online form filling, bill sourcing and payments, or complex applications like distance education and tele-medicine.

Shivaji Chatterjee, senior director, sales and marketing, Hughes Escorts Communications says, "IT has a vital role to play in all transactions that the government undertakes. It helps the government cut red-tapism, avoid corruption, and reach citizens directly." He points out that such initiatives will help citizens learn about the various policies, processes and help-lines that the government offers. The governments of Singapore, Canada and Switzerland have implemented such portals, and set the benchmarks in this regard. With the help of IT, the government can process citizen to government transactions such as the filing of tax returns, death and birth registration, land records, etc.

Rajiv Kaul, managing director, Microsoft India adds "A strong technology infrastructure can help central and state governments deliver a comprehensive set of services to citizens." Microsoft is working with several state governments to help evolve a long-term technology blueprint for IT infrastructure. It is working with various departments of the central government, and has undertaken several projects and initiatives with state governments as well.

Manoj Kunkalienkar, Executive Director, ICICI Infotech says, "As far as e-governance projects are concerned, the government is gradually changing its role from an 'implementer' to a 'facilitator and regulator.' It will encourage private sector participation in e-governance projects, so more projects in e-governance based upon the public private participation (PPP) model should come about in the near future."
Agriculture, power and education are fields where the government makes use of IT to provide services to citizens. The revenue collection department is in the process of using information technology for applications such as income tax. Some notable examples:

- A Kolkata-based hospital leverages e-governance for tropical medicine. The hospital employs tele-medicine to assist doctors in rural areas as they analyse and treat panchayat residents. This method does away with patients having to travel all the way to Kolkata for treatment. Patients feel better being examined in their own village. Using tele-medicine, the hospital is able to dispense its expertise to far-flung districts. The patient goes for an examination to the local doctor in the panchayat. This doctor is in contact via a voice & data connection with a doctor at the hospital for tropical medicine. Thus, the panchayat resident gets the benefit of being treated by both a local doctor and a hospital specialist.

- The Karnataka government’s ‘Bhoomi’ project has led to the computerisation of the centuries-old system of handwritten rural land records. Through it, the revenue department has done away with the corruption-ridden system that involved bribing village accountants to procure land records; records of right, tenancy and cultivation certificates (RTCs). The project is expected to benefit seventy lakh villagers in 30,000 villages. A farmer can walk into the nearest taluk office and ask for a computer printout of his land record certificate for Rs 15. He can also check details of land records on a touch-screen kiosk by inserting a two-rupee coin. These kiosks, installed at the taluk office, will provide the public with a convenient interface to the land records centre.

- In Gujarat there are websites where citizens log on and get access to the concerned government department on issues such as land, water and taxes.

- In Hyderabad, through e-Seva, citizens can view and pay bills for water, electricity and telephones, besides municipal taxes. They can also avail of birth / death registration certificates, passport applications, permits / licences, transport department services, reservations, Internet and B2C services, among other things.

- eChoupal, ITC's unique web-based initiative, offers farmers the information, products and services they need to enhance productivity, improve farm-gate price
realisation, and cut transaction costs. Farmers can access the latest local and global information on weather, scientific farming practices, as well as market prices at the village itself through this web portal—all in Hindi. eChoupal also facilitates the supply of high quality farm inputs as well as the purchase of commodities at the farm.

Given the literacy and infrastructure constraints at the village level, this model is designed to provide physical service support through a choupal sanchalak—himself a lead farmer—who acts as the interface between the system and the farmers. The contents of this site in their entirety are made available only to the registered sanchalaks.

Kunkalienkar says that from a political perspective, after watching the performance of some IT-savvy states in the recent elections, the system has woken up to the need to focus more on rural development. "The political systems are keener to use IT to disseminate information faster to farmers, disburse loans, improve education and the health systems in villages, etc. There is a clear-cut incentive to do it as 60 percent of the vote-bank still lives in rural India."

Chatterjee says that e-governance has to be supported by the will and resources of those who are in governance, be it at the central or state level. The central government has analysed and appreciated the concept by creating a separate e-governance department headed by a secretary to trigger e-governance in India. The World Bank, ADB and UN have been approached, and in response they are generously funding e-governance projects.

In future, education, agriculture, state wide area networks (SWANs) and Community Information Centre projects will be rolled out backed by a strong public private participation model (PPP) to achieve long-term sustainability.

Projects with PPP models in these segments can revolutionise the governance experience. In the next couple of years the industry is expected to grow by 22-25 percent.
While one appreciate, therefore, the good match between IT as an appropriate tools or better governance, we must also take note of certain other aspects which applying IT of better governance. The first is the role of the vested interests. We have seen how government systems are corrupt and delay in turn breeds corruption. There will always be people who benefit from the present system and who will oppose the introduction of IT. The second aspect to be borne in mind is that there is an element of techno-phobia about IT among many govt. employees. This can easily be overcome because computers are all the time, are becoming more user friendly.

The third aspect is that the computers are seen as job eaters but the improvement in production they bring may help so increase the jobs. We have seen for instance, how even though the workload had increased by 100% computerised railway reservation system has resulted substantial railways. A study made in Delhi shows that in the investment made in computers has yielded returns within a year itself in terms of saving time, of the people at large, the speed for pro reservation and so on.

A fourth aspect of IT to be noted when it comes to apply to the government is the need for attending the laws so that the government runs today on paper can also run on IT. Government of India committee under the Chairmanship of secretary, electronics which has submitted its recommendations about the cyber laws. The interim report before the government.

If we look at the implications of IT in Governmental, perhaps after the success of railway reservation system, the most exciting development is the initiative taken by the CM of Andhra Pradesh, Shri Chandrababu Naidu to give push to IT in the government. The government has adopted a very comprehensive strategy of first improving the infrastructure by going govt. for the APNet. Ultimately the govt. has adopted the policy which would attract MNCs and their leading players in IT so that the manpower which is needed for this technology is developed in the state. The setting up of the high tech city is an excellent example of this enlightenment approach. Systematically in areas like
registration office and so on, computerisation has been introduced. Andhra Pradesh can be a model of what can be done by a state to bring better quality of life to the people at large.

There may be other examples in other states where IT has been used effectively. So, if we want to use IT more efficiently in Govt. we will have to perhaps learn from successful experience and try to replicate to the extent possible. There is no point in reinventing the wheel. Here I would suggest that successful govt. should adopt more liberal and not purely an account oriented approach so that the software and the technique available with them can be successfully used elsewhere.

A look at the pre-conditions needed today to make IT in Govt. more effective will not out of place. First, what is needed is a political will. Chandrababu Naidu, CM of Andhra Pradesh is an example of how political will can help. Fortunately the national agenda for governance of the govt. of India has also recognized the importance of IT. Therefore, we can take it that today there is political will not apply IT in govt. the Prime Minister also announced a few days ago that the national task force would set or IT to make India into a Software power. The increasing realization of significance of IT by the political leaders is a healthy development.

While the political leadership can only provide a direction, ultimate implementation depends on the bureaucracy. It is here the bureaucracy will have to learn from the excellent leadership provided by successful bureaucrats in states like Andhra Pradesh, the railway board and elsewhere so that the entire movement for greater application of IT can be given a push. The govt. set up many years ago the National Information Centr (NIC). So we have in NIC a dedicated organisation to bring IT in govt. But, while NIC will have the technical expertise, unless the user departments are able to appreciate the use of IT, no success is possible.

Equally important is the issue of affordability of IT systems. A three point formula is suggested to make the IT more affordable and also use it successfully for changing the way government is run. The first point is that at least 2% of the every departments
budget should be earmarked for using IT in the department. Secondly, the budget should provide that a 190% depreciation in the first year itself for investment in IT. Thirdly, effective implementation of cyber laws so that application of IT is not stymied on legal grounds. A model is also developed for the postal department for totally computerising it in the next two to five years. Similar exercises are being done for other departments but what is important is implementation.

Government ultimately exists for national development. What can be done to bring IT in the nation at large. The eminent administration expert Paul Appleby who studied Indian administration said that Indian administration was action shy. The IT can be excellent, tool for, transforming the government into a more responsive and effective organisation. Especially as we are on the eve of the 21st Century. It is a challenge to the bureaucrats to see that this revolution is brought about.

A review of the status of computerization shown that while much work has been done in introducing computers within the Govt., much more needs to be done in order to increase the availability and use of computers.

2.4 ORGANISATIONAL AND HUMAN RESOURCE DEVELOPMENT

The policy aspects related to organizational and human resource development can be summarized as under:

Greater involvement of Ministries
The Ministries need to have a much greater involvement in the pro Part of this can be facilitated by ensuring that they have a five year plan for information Technology and a specific provision is made for computerization that there is a clear goal and the resource to achieve it are available. The have more formal control of the NIC staff working under
them through a System in which a section of the ACR of the NIC unit head is written by a nominee the Chairman of the NMCC in which the NIC officer is posted. Similarly the of the NIC unit avail of leave only with the concurrence of the nominee of the NMCC.

**Spreading Awareness of IT**

In order to increase the awareness of the need for IT effectively, in every department there have to be wide ranging workshops and seminars involving all levels of administration form the highest to the lowest preferably in the model of vertical integration courses in IAS. This will help in demystifying IT, identifying the real needs of IT, using of IT profitably and also to create an atmosphere which will be friendly and conducive for inclusion of IT culture. Such an effort has never been made in the past and that is one of the reasons why the progress of IT in the Govt is not as it should be inspite of the sheer and massive efforts made by NIC.

**Increasing availability of Computers**

In order to spread the IT culture restrictions regarding the level at which the computers can be permitted should be removed. There are restrictions in some departments that offices of certain level and above only are entitled to computers. In fact computers should be available to any government servant who is, interested in IT. They should also be permitted to install computers in their homes. If necessary that the culture of computers will grow. As this will involve a major expenditure on the part of government, if government has to pay upfront, the strategy of getting the computers on lease can be thought of. In order to bring down the lease costs, the income tax may be amended so that any investment made in computers and IT systems becomes eligible for 100% depreciation in the first year itself. Such concession given in the case of wind farms have resulted in the wind farms being available through leasing companies at 12% interest. A similar exercise would help not only reducing the government outgo but also indirectly catalyse the IT revolution both within the government and outside.
Changing recruitment qualifications

Certain changes in the qualifications for recruitment of employees so as to employ persons with keyboard skills combined with the required levels of computer training and as a system of incentives would go a long way in ensuring that employees have the requisite skills for effectively using computers.6.5 identifying Mentors: Secretaries of Ministers must identify suitable persons with an aptitude for computers who can perform the role of leaders and mentors in spreading the culture of IT not only in the Ministry but also in subordinate organisations. Govt should freely allow officers if the level of Deputy Secretaries and above to have computers at their residence also. These computers should be networked so that an effective intranet within the govt grows.

2.5 PERSONAL MANAGEMENT SYSTEM

A review of the status of computerisation of the personnel management systems has shown that it is necessary for a small group of officers to be constituted in the Department of Personnel and Training to design the specific databases which would form a comprehensive but modular Personnel information for use for personnel management across cadres and levels. The issues of confidentiality and privacy would have to be suitably addressed. Each Ministry/Department must allocate 2 to 3% of its Budget for spending on IT so that there is an increase in the availability of funds for training in IT an acquisition of hardware, software as well as for the development of software and maintenance.

2.6 DELIVERY OF SERVICES

Objectives:
The long-term objective should be to provide an electronic one-stop-shop for Government services available 24 hours a day, seven days a week. Government services provided to the public should be charged for from the beginning as introducing charges later may create difficulties.
Phasing:
The delivery of services could be implemented in three phases. In the first phase the delivery would be in the front offices of Government departments. In the next this could be through information kiosks/manned public access terminals located in remote locations such as post offices, railway stations, hospitals, milk booths. In the third phase the points of usage could be extended to PCOs which could ensure 24 hour operations. They could provide value added services such as Internet access for email.

Government Intranet:
For operationalising this it would be necessary for the Government departments to build up computerised information bases which can be interconnected. These could be on an intranet which would not only facilitate access within the Government but also enable, easy connectivity to enable others outside the Government to gain access to the Information. In order to avoid misuse there would have to be appropriate security safeguards.

Co-ordination:
In the report a number of suggestions have been made for increasing the finances available for IT providing a scope for Initiative by the different departments for using IT and also optimizing the resources of NIC. The Committee is of the view that a high powered committee under the Chairmanship of Cabinet Secretary should be set up to improve administrative efficiency by using information technology in Government. The members of this committee could include the Department of Administrative Reforms, NIC and representatives of some Ministries.

2.7 CYBER LAWS

With the increasing use of Information technology it will be necessary to make appropriate amendments of existing laws so that the advantage of the technology are not negated by the obsoleteness of laws.
The Information Technology (IT) Act, 2000

The Information Technology (IT) Act, 2000 which came into force on 17th October, 2000 covers the law related to information technology, which is mainly based on the model law enunciated by the United Nations Commission on International Trade Law (UNCITRAL) on Electronic Commerce in 1996, which provides for equal legal treatment of users of electronic communication and paper based communication.

The Act has been designed to give boost to Electronic Commerce (e-commerce), e-transactions and similar activities associated with commerce and trade, and also to facilitate electronic Governance (e-governance) by means of reliable electronic records.

Objects of IT Act

The objects of the IT Act as set out in the “Statement of Objects and Reasons” appended to the “Information Technology Bill, 2000,” reads as under:

“New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Businesses and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages. It is cheaper, easier to store retrieve and speedier to communicate. Although people are aware of these advantages, they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements as to writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents and records which should bear signatures. The law of evidence is traditionally based upon paper based records and oral testimony. Since electronic commerce eliminates the need for paper based transactions, hence to facilitate e-commerce, the need for legal changes
have become an urgent necessity, International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

"There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures. This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium.

"With a view to facilitate Electronic Governance, it is proposed to provide for the use and acceptance of electronic records and digital signatures in the Government offices and its agencies."

Scope of IT Act
The Information Technology Act, 2000 consists of 13 Chapters divided into 94 Sections. Chapters I to VIII are related to law on digital signature. Chapters IX to XIII cover penalties, offences, etc. The Act also contains four Schedules incorporating consequential amendments in respect of certain other Acts.

- **First Schedule** makes amendments to the Indian Penal Code, 1860,
- **Second Schedule** makes amendments to Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
- **Third Schedule** makes amendments to the Banker’s Book Evidence Act, 1891 to give legal sanctity for books of accounts maintained in the electronic form by the banks.
- **Fourth Schedule** makes amendments to the Reserve Bank of India Act, 1934 to facilitate electronic fund transfers between the financial institutions and banks.
Application of the Act
As provided under Sec 14, the provisions of the IT Act, 2000 shall not apply to the following documents:

1. Execution of a Negotiable Instrument under the Negotiable Instruments Act, 1881.
3. Creation of a Trust under Indian Trusts Act, 1882.
4. Execution of a ‘Will’ under the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
6. Execution of such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

A brief Review of the Law on Information Technology is presented as follows:

DIGITAL SIGNATURE

Digital signatures are the electronic equivalent of the handwritten signatures. Since in an electronic message or transaction affixing handwritten signature is not possible, authentication has to be achieved by some electronic or digital method. Digital signatures facilitate this authentication.

Digital signature means authentication of any electronic record by a subscriber, i.e., a person in whose name the “Digital Signature Certificate” is issued, by means of an electronic method or procedure in accordance with the provisions of Section 3.

Affixing digital signature means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of “digital signature”.

Sec 3 provides that any subscriber may authenticate an electronic record by affixing his digital signature. The authentication of the electronic record shall be effected by the use
of ‘asymmetric crypto system’ and ‘hash function’, which envelop and transform the initial electronic record into another electronic record.

"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 drive or reconstruct the original electronic record from the hash result produced by the algorithm;

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

Any person by the use of public key of the subscriber can verify the electronic record. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

In the case of electronic transmission of business or legal message/documents it is necessary to ensure that these are authentic and have not been tampered with by any person during transmission. With this end in view, the above stated Section 3 provides that authentication of the electronic record is to be effected by the use of “asymmetric crypto system”, i.e. by using ‘encryption’ (coding) and ‘decryption’ (decoding) methodologies and software tools.

**Encryption software programme**

An ‘encryption software programme’ takes the normal, readable text message (“plaintext”) and scrambles the message into unreadable coded text or “ciphertext”. The recipient then uses another software program (the corresponding decryption program) to decrypt such ciphertext back into normal plaintext. Any one who intercepts the message will, therefore, not be able to read or tamper with the message, unless he has the key, i.e., the corresponding decryption program, thereby rendering it secure.
Asymmetric crypto system

Asymmetric crypto system means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

In "asymmetric crypto system", each person will have two corresponding and matched keys – one called the 'private key' which is always kept secure with such person, and the other called the 'public key' which the person shares with others and makes available to others on specialized databases called 'repositories' or through Certification Authorities.

These two keys, public key and private key, are used to encrypt and decrypt the message respectively. The sender uses the intended receiver's public key (which he can freely obtain from the receiver or download from a public repository) to encrypt the message. The receiver, on receiving the coded message, uses his corresponding private key (which is available only with him) to decrypt the encrypted message. The public key and the private key of any person or entity would be so mathematically linked that a message encrypted using one key can only be decrypted by using the corresponding other.

ELECTRONIC GOVERNANCE

IT Act, 2000 facilitates electronic governance to accord legal recognition to electronic records, digital signatures and electronic form of dealing with Government offices and its agencies. The following provisions are thus, contained in the Act:

Legal Recognition of Electronic Records

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

(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference
Legal Recognition of Digital Signatures
Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person the notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Use of Electronic Records and Digital Signatures in Government and its Agencies
Where any law provides for –
(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;
(c) the receipt or payment of money in a particular manner the, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied in such filing, issue of grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

The appropriate Government may, by rules, prescribe –
(a) the manner and format in which such electronic records shall be filed, created or issued;
(b) the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record under Clause (a) stated above.

Retention of Electronic Records
Where any law provides that documents, records or information shall be retained for any specific period, then that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form –
(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record.

However, the above rule does not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. Further, the Section shall not apply to any law that expressly provides for the retention of documents, records of information in the form of electronic records.

Publication of Rules, Regulations, etc., in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or electronic Gazette.

However, where any rule, regulation, order, byelaw, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

No Right to insist that the Document should be accepted in Electronic Form

Sections 6, 7 and 8 shall not confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.
Central Government empowered to make Rules in respect of Digital Signature

The Central Government is empowered to make rules in respect of digital signature prescribing—

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

The Central Government has notified the “Information Technology (Certifying Authorities) Rules, 2000. Rule 3 of these Rules provides the manner in which the information is to be authenticated by means of digital signature. Rule 4 provides the manner of creation of digital signature, and Rule 5 provides the manner of verification of digital signature.

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

Under this heading, the IT Act, 2000 contains provisions regarding—

(a) when the transmission of an electronic record shall be attributed to the originator?
(b) would the addressee/receiver be bound to acknowledge the receipt of that electronic record?; and
(c) how to determine the time and place of dispatch and receipt of electronic record?

Attribution of Electronic Records

An electronic record shall be attributed to the originator, if it was sent—

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

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

Acknowledgement of Receipt

No agreement. Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by –

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

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

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

No stipulation by the originator. Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may given notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent [Sec. 12(3)].
**Time and Place of Despatch and Receipt of Electronic Record**

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

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

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records –
   (i) receipt occurs at the time when the electronic record enters the designated computer resource; or
   (ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee [Sec. 13(2)].

Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business [Sec. 13(3)].

The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3) [Sec. 13(4)].

For the purposes of this Section –

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;
(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
(c) "usual place of residence", in relation to a body corporate, means the place where it registered [Sec. 13(5)].

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

IT Act, 2000 lays down the legal presumptions as to when the 'electronic record' and 'digital signature' are deemed secure as the communicated electronic records and messages must be secure and reliable for giving boost to e-commerce.

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.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was –

(a) unique to the subscriber affixing it;
(b) capable of identifying such subscriber;
(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including:

(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and  
(f) the procedures in general use for similar types of transactions or communications.

REGULATION OF CERTIFYING AUTHORITIES

IT Act, 2000 provides for the appointment, functions, powers and duties of “Controller of Certifying Authorities” and other officers.

Appointment of Controller and other Officers

Sec 17 provides as follows:

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, deputy Controllers and Assistant controllers shall be such as may be prescribed in the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

Functions of Controller

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

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

(b) certifying public keys of the Certifying Authorities;
(c) laying down the standards to be maintained by the Certifying Authorities;
(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
(g) specifying the form and content of a Digital Signature Certificate and the key;
(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(l) resolving any conflict of interest between the Certifying Authorities and the subscribers;
(m) laying down the duties of the Certifying Authorities;
(n) maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations which shall be accessible to public.

Recognition of Foreign Certifying Authorities
Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act [Sec. 19(l)].
Where any Certifying Authority is recognized under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of the Act [Sec. 19(2)].

*Revocation of recognition.*

The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recoded in writing, by notification in the Official Gazette, revoke such recognition [Sec. 19(3)].

**Controller to Act as Repository**

A ‘repository’ is an online database of Digital Signature Certificates and other related information useful for those who conduct their business operations through the medium of computer internet or e-commerce. The Controller shall be the repository of all Digital Signature Certificates issued under this Act [Sec. 20(1)].

To ensure that the secrecy and security of the digital signatures are assured the controller shall –

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

(b) observe such other standards as may be prescribed by the Central Government [Sec. 20(2)].

The Controller shall maintain a computerized database of all public keys in such a manner that such database and the public keys are available to any member of the public [Sec. 20(3)].

**Grant of Licence to Certifying Authorities to Issue Digital Signature Certificates**

Any person may make an application, to the Controller, for a licence to issue Digital Signature Certificate, provided he fulfils such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are
revocation, as the case may be, shall be made available through a website which shall be accessible round the clock.

**Powers of Controller**

The Controller of Certifying Authorities has the following powers:

1. Power to authorize, in writing, the Deputy or the Assistant Controller or any officer to exercise any of his powers (Sec. 27).

2. Power to take up for investigation any contravention of the Act or rules or regulations made thereunder. He may authorize any officer also in this behalf [Sec. 28(1)].

3. Power to exercise himself or through an authorized officer like powers which are conferred on Income-tax Authorities under Chapter XIII of the Income-tax Act, 1961 [Sec. 28(2)]. A few such powers are briefly stated below:
   (i) Powers as are vested in the Court when trying a suit in respect of matters relating to inspection, enforcing attendance of any person and examining him on oath, compelling the production of books of account, etc.
   (ii) Power to enter and search any building, place, etc., where books of account, documents or valuables are believed to be kept, and seize them.
   (iii) Power to requisition books of account or assets from any officer possessing them.
   (iv) Power to call for information.
   (v) Power to inspect and take copies of any Register of Members or Debentureholders.
   (vi) Power to make enquiries.

4. Power to direct, by order, a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order, if those are necessary to ensure compliance with the provisions of the Act, rules or any regulations made thereunder [Sec. 68(1)].

5. Power to direct, by order, any agency of the Government to intercept any information transmitted through any "computer resource" (i.e., computer, computer system and computer network, etc.), if it is necessary or expedient in the
interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commissioner of any cognizable offence [Sec. 69(1)].

Access to Computers and Data
If the Controller has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, the Controller or any other person authorized by him shall have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. He may also, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Certifying Authority to follow certain Procedures The person to whom a licence has been granted by the Controller to issue Digital Signature Certificates is termed as a Certifying Authority [Sec. 2(1)(g)].

Every Certifying Authority shall follow certain procedures relating to security of system, in performance of its services. It is required, to,-

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

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

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

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

Duties of Certifying Authority
The Certifying Authority has the following duties:
1. To ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of the Act, rules, regulations and orders made thereunder (Sec. 31).

2. To display its licence at a conspicuous place of the premises in which it carries on its business (Sec. 32).

3. To surrender the licence to the Controller immediately after its suspension or revocation [Sec. 33(1)].

4. To disclose in the manner specified by the regulations –
   (a) its Digital Signature Certificate which contains the public key corresponding to the private key used by the Certifying Authority to digitally sign another Digital Signature Certificate;
   (b) any certification practice statement relevant thereto;
   (c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
   (d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority’s ability to perform its services [Sec. 34(1)].

5. To make reasonable efforts to notify any person who is likely to be affected by the occurrence of any event which, in the opinion of the Certifying Authority, may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted. He may also act in accordance with the procedure specified in its ‘certification practice statement’ to deal with such event or situation [Sec. 34(2)].

DIGITAL SIGNATURE CERTIFICATES

The purpose of a digital signature certificate is to authenticate the identity of an individual. It ensures that the purported send is in fact the person who sent the message. The Certifying Authority signs it digitally.

Certifying Authority to Issue Digital Signature Certificate
Application. Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government. The application shall be accompanied:

(a) by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government. However, different fees may be prescribed for different classes of applicants,

(b) by a ‘certification practice statement’ or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

**Grant of certificate**

On receipt of an application for the issue of Digital Signature Certificate, the Certifying Authority may, after consideration of the ‘certification practice statement’ or the other statement referred above and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application. However, no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that:

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

**Representations upon issuance of Digital Signature Certificate**

While issuing a Digital Signature Certificate, the Certifying Authority certifies that the information contained in it is accurate and that:

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;

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

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
(d) the subscriber's public key and private key constitute a functioning key pair; and
(e) it has no knowledge of any material fact, which if it had been included in the
Digital Signature Certificate would adversely affect the reliability of the
representations made in clauses (a) to (d).

**Suspension of Digital Signature Certificate**
The Certifying Authority which has issued a Digital Signature Certificate may suspend
such digital Signature Certificate, -

(a) on receipt of a request to that effect from –
   (i) the subscriber listed in the Digital Signature Certificate or
   (ii) any person duly authorized to act on behalf of that subscriber;
(b) if it is of opinion that the Digital Signature Certificate should be suspended in
   public interest.

A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days
unless that subscriber has been given an opportunity of being heard in the matter. Further,
on suspension of a Digital Signature Certificate under this Section, the Certifying
Authority shall communicate the same to the subscriber.

**Revocation of Digital Signature Certificate**
A Certifying Authority may revoke a Digital Signature Certificate issued by it –

(a) where the subscriber or any other person authorized by him makes a request to
    that effect; or
(b) upon the death of the subscriber; or
(c) upon the dissolution of the firm or winding up of the company where the
    subscriber is a firm or a company.

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

(a) a material fact represented in the Digital Signature Certificate is false or has been
    concealed;
(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
(c) the Certifying Authority’s private key or security system was compromised in a manner materially affecting the Digital Signature Certificate’s reliability;
(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter. Further, on revocation of a Digital Signature Certificate under this Section, the Certifying Authority shall communicate the same to the subscriber.

**Notice of suspension or revocation**

Where a Digital Signature Certificate is suspended or revoked under Section 37 or Section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice. Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

**DUTIES OF SUBSCRIBERS TO DIGITAL SIGNATURES**

The IT Act, 2000 lays down the following duties of the subscribers who have obtained the Digital Signature Certificate from some Certifying Authority.

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

2. **Acceptance of Digital Signature Certificate**

   A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes its publication:
   
   (a) to one or more persons;
(b) in a repository, or
(c) If he otherwise demonstrates his approval in any manner.

3. **Subscriber representation.**

By accepting a Digital Signature Certificate the subscriber certified to all who reasonable rely on the information contained therein that—

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

(b) all his representations to the Certifying Authority and all material relevant information contained in the Certificate are true;

(c) all information in the Certificate that is within his knowledge is true.

4. **Control of Private Key**

Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix his digital signature. If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in the prescribed manner. Till so communicated, he shall be liable.

**PENALTIES AND ADJUDICATION**

The following provisions are made with regard to penalties and adjudication:

**Penalty for Damage to Computer, Computer System, etc.**

If any person indulges in any of the following acts, without permission of the owner or any other person who is in charge of a computer, computer system or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected:

(a) accesses or secures access to such computer, computer system or computer network;
(b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or date held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(h) charges the services availed of by a person to the account of another person by tampering with a manipulating any computer, computer system, or computer network.

For the purposes of this Section —
(i) "computer contaminant" means any set of computer instructions that are designed —
(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system or computer network;
(ii) "computer database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

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

Penalty for Failure to Furnish Information, Return, etc.
If any person who is required under this Act or any rules or regulations made thereunder to--

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

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

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

Penalty Where No Specific Penalty is Provided Elsewhere in the Act
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.
Adjudication – Appointment of Adjudicating Officer

For the purpose of adjudging whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government. However, no person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

The adjudicating officer shall, after giving the person referred to above, give a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that Section.

Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

Powers. Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of Section 58, and –

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860;
(b) shall be deemed to be civil court for the purposes of Section 345 and 346 of the Code of Criminal Procedure, 1973.

Factors to be taken into account by the Adjudicating Officer

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

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
(b) the amount of loss caused to any person as a result of the default;
(c) the repetitive nature of the default.

THE CYBER REGULATIONS APPELLATE TRIBUNAL

IT Act, 2000 deals with the establishment of one or more Appellate Tribunals to be known as Cyber Regulations Appellate Tribunal or Cyber Appellate Tribunal to exercise jurisdiction, powers and authority as conferred under the Act.

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

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit. The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer. The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he –
(a) is, or has been, or is qualified to be, a Judge of a High Court or
(b) is or has been member of the Indian Legal Service and is holding or has held a post in Grade I of the Service for at least three years.

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

The Presiding Officer of Cyber Appellate Tribunal may, be noticed in writing under his hand addressed to the Central Government, resign his office. However, he shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges. The Central Government may, be rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.
Appeal to Cyber Regulations Appellate Tribunal

Any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. However, no appeal shall lie from and order made by an adjudicating officer with the consent of the parties.

Period allowed for appeal. 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 the 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 Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

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

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal (Sec. 59).

Power of the Cyber Appellate Tribunal

The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908. It shall, however, be guided by the principles of natural justice, provisions of the Act and rules made thereunder. Natural justice means to act in good faith, fairly, justly and impartially and never arbitrarily. It shall have power to regulate its own procedure including the place at which it shall have its sittings.
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, while trying a suit, in respect of the following matters, namely:

(a) summoning and enforcing the attendance of any person and examining him on oath.
(b) requiring the discovery and production of documents or other electronic records;
(c) receiving evidence on affidavits;
(d) issuing commissions for the examination of witnesses or documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex parte;
(g) any other matter which may be prescribed.

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

The Adjudicating Officer and the Cyber Appellate Tribunal have exclusive jurisdiction to decide specific issues for which they have been empowered. Section 61 provides that:

(a) No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine; and
(b) No injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act. Injunction is a specific order of the court directing the defendant to refrain from doing certain act.
Appeal to High Court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact of law arising out of such order. However, the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

Compounding of Contraventions

Any contravention under the Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions he may impose. However, the compounded sum shall not, in any case, exceed the maximum amount of penalty which may be imposed under this Act for the contravention so compounded.

The above provision shall not apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention committed by him, was compounded.

Here any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

Where any contravention has been compounded, no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.
Recovery of Penalty
A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital signature Certificate, as the case may be, shall be suspended till the penalty is paid.

OFFENCES
Section 65 to 76 of the IT Act deal with criminal penalty, which are discussed as under:

Tampering with Computer Source Documents
If any person 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, he shall be punishable with imprisonment up to three years, or with fine up to two lakh rupees, or with both.

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

Hacking with Computer System
Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine up to two lakh rupees, or with both.

Publishing of Information, which is Obscene in Electronic Form
Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be
punished. On first conviction he shall be punishable with imprisonment up to five years and with fine up to one lakh rupees. In the event of a second or subsequent conviction he shall be punishable with imprisonment up to ten years and also with fine up to two lakh rupees.

It may be noted that it is only the publishing or transmitting of obscenity, which is an offence, and not its possession.

**Securing Unauthorised Access to the Protected System**

The Government, may by notification in the Official Gazette declare that any computer, computer system or computer network to be a protected system. It may also, by order in writing, authorize persons to have access to it. Any person who secures or attempts to secure unauthorized access to a protected system shall be punished with imprisonment, which may extend to ten years and shall also be liable to fine.

**Penalty for Misrepresentation**

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital 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.

**Penalty for Breach of Confidentiality and Privacy**

If any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person, he 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. Thus, Section 72 prohibits unauthorized disclosure of the contents of electronic record.
Penalty for Publishing Digital Signature Certificate or otherwise make it available to any other person with the knowledge that:

(a) it has not been issued by the Certifying Authority; or
(b) it has not been accepted by the subscriber; or
(c) the certificate has been revoked or suspended.

However, if the publication is for the purpose of verifying a digital signature created prior to such suspension or revocation, this rule will not apply.

Any person, who contravenes the above 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.

**Publication for Fraudulent Purposes**

Whoever knowingly creates, publishes or otherwise makes available a Digital 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.

**Act to Apply for Offence or Contravention Committed Outside India**

The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**Confiscation**

Section 76 provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of which there is contravention of any provision of this Act.
However, where it is established to the satisfaction of the court adjudicating the confiscation that the person who is in possession, power or control of these articles in not responsible for the contravention, the court may, instead of making an order for confiscation, make such other order as it may think fit.

**Penalties and Confiscation not to Interfere with other Punishments**

Any penalty imposed or confiscation made under this Act shall not interfere with other punishments provided under any other law for the time being in force.

**Power to Investigate Offences**

A police officer not below the rank of Deputy Superintendent of Police is empowered to investigate any offence under this Act.

**Network Service Providers not to be Liable in Certain Cases**

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

**Offences by Companies**

Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is 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, unless he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention. If it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, and director, manager, secretary or other officer of the company,
such person shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

**Constitution of Advisory Committee**

The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee. It shall consist of a Chairperson and such number of other official and non-official members representing the interest principally affected or having special knowledge of the subject-matter as the Central Government may deem fit. There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

The Cyber Regulations Advisory Committee shall advise –

(a) the Central Government either generally as regard any rules or for any other purpose connected with the Act;

(b) the Controller in framing the regulations under this Act.

The Central Government has notified the constitution of “Cyber Regulations Advisory Committee” consisting of 21 members including the Chairperson vide Notification No. GSR 790(E), dated 17th October, 2000.

**2.8 IT INDUSTRY IN INDIA**

The Indian IT industry is broadly categorised into IT services and software, ITES-BPO and Hardware segments.

The industry continues to chart remarkable double-digit growth, with industry aggregate revenue for 2004-05 expected to reach US$ 28 billion. The industry is forecast to grow more than fivefold over FY 1998-05, at a CAGR of 28 percent.

The industry’s contribution to the national economic output has nearly tripled – from 1.2 percent in FY 1997-98 to 3.5 percent in FY 2003-04. This sector is forecast to grow at
nearly 31 percent this fiscal to account for an estimated 4.1 percent of the national GDP in FY 2004-05.