12 CYBER LAWS

INTRODUCTION

- Technology has proved to a great leveler. It has helped in creating 'machine - clones' in the form of computers a high speed data processing device performing arithmetic, logical and memory functions by manipulating optical, magnetic and electrical impulses.
- The power of one 'machine-clone' is power of all connected 'machine- clones', which may be termed as network - of - network or Internet.
- This dynamic virtual space created by the networks of 'machine-clones' has been termed as cyber space.
- The word Cyberspace first appeared in 'William Gibson's' in his science fiction Necromancer published in 1984.
- Gibson portrayed cyberspace as a three dimensional virtual landscape created by network computers.
- The New Oxford Dictionary of English defines 'Cyberspace' as the notional environment in which communication over computer networks occur.
- Cyber space is a virtual medium.
- It has no boundaries, no geographical mass or gravity.
- It exists in a form of bits and bytes.

CYBER SPACE VS. PHYSICAL WORLD

	Cyber Space	**Physical World**
1.	It is a digital medium.	It is a physical world
2.	It is static, well defined and incremental.	Cyber space is dynamic, undefined and exponential.
3.	The contours of cyber space is as vast as human imagination and thus cannot be given a fixed shape.	The contours of physical world are fixed.

4.	Cyber space represents network of millions of computers creating **specter of digital life.**	It does not represent any network.

CYBER LAWS

- When the concept of Internet was founded and later developed little did the developers know that the internet would have the power of being transformed into a monster that could be used for several illegal and immoral activities and it would eventually need to be regulated.
- There are several disturbing things that happen in cyberspace ranging from identity theft and terrorism to money laundering. These grey areas create a need for cyber laws.
- Various criminals like hackers; crackers have been able to pave their way to interfere with the internet accounts through Domain Name Server (DNS), Internet Provider's address (IP), spoofing, phishing, internet phishing, etc. to gain unauthorised access to user's computer system and steal data to make profits.
- There is no clear definition of cyber law, computer law or Information and communication technology law.
- Cyber law is a term concerning the legal issues related to the use of communicative, transactional and distributive aspects of networked information devices and technologies.
- Cyber law encompasses the legal, statutory and constitutional provisions that affect computer and computer networks. It concerns individuals, corporate bodies and institutions which

  1. Are instrumental for the entry into cyberspace,
  2. Provide access to cyberspace,
  3. Create hardware and software which enable people to access cyberspace and,
  4. Use their own computers to go "online" and enter cyberspace.
- It is a generic term which refers to all the legal and regulatory aspect of internet and World Wide Web.
- There are currently two main Statures, which govern online criminal liability- the Indian Penal Code, 1860 and the Information Technology (IT) Act, 2000.

- The main objective of the Act is to regulate and control the affairs of cyber world in an effective manner.

INFORMATION TECHNOLOGY ACT 2000

- India is the 12th nation in enactment of cyber law with the passage of Information Technology Act, 2000.
- The United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce in 1996 in order to bring uniformity in the law of different countries.
- The first draft of legislation was created by the Ministry of Commerce, Government of India as E commerce Act 1998.
- A redraft of legislation was prepared as "Information Technology Bill 1999" which was placed before the Parliament in December 1999 and passed in May 2000.

AIM AND OBJECTIVES OF THE ACT

1. To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred as e-commerce in place of paper based method of communication,
2. To give legal recognition to digital signature for authentication of any information or matter which requires authentication under any law,
3. To facilitate electronic filling of documents with Government departments,
4. To facilitate electronic storage of data,
5. To facilitate and give legal sanction to electronic fund transfer between banks and financial institutions,
6. To give legal recognition for keeping books of accounts by bankers in electronic form under the Evidence Act 1891 and the Reserve Bank of India Act 1934.

FEATURES OF THE ACT

1. Electronic contracts have been made legally valid if made through secure electronic communications
2. Legal recognition has been granted to digital signatures

3. Security procedures for electronic records and digital signature have been laid down
4. A procedure for appointment of adjudicating officers for holding inquiries under the Act has been laid down
5. A provision has been made for the establishment of Cyber Regulatory Appellant Tribunal under the Act
6. An appeal against the order of the Controller or Adjudicating officer can be made to Cyber Appellant Tribunal and not to any civil court
7. Appeals against order of the Cyber Appellant Tribunal are to be made in the High court
8. Digital signatures are to be effected by use of asymmetric crypto system and hash function
9. A provision has been made for appointment of Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities
10. The controller is to act as repository (a storehouse, that is who will maintain an authentic and complete information) of all digital signature certificates
11. The Act is to apply to offences or contraventions committed outside India
12. Senior police officers and other officers have been given power to enter any public place and search and arrest without warrant
13. Provisions have been made for the constitution of a Cyber Regulations Advisory Committee to advice the Central Government and the Controller.

APPLICABILITY AND NON- APPLICABILITY OF THE ACT

- The Act extends to the whole of India, including Jammu and Kashmir.
- The Act can be applied to any offence or contravention committed outside India by any person irrespective of his/her nationality, if his/her conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Non Applicability

1. Execution of Negotiable Instrument under Negotiable Instruments Act, 1881 except cheques.

2. Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
3. Creation of Trust under Indian Trust Act, 1882.
4. Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition.
5. Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

BASIC DEFINITIONS

Access	It means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network.
Addressee	It means a person who is intended by the originator to receive the electronic record but does not include any intermediary.
Adjudicating Officer	It means an adjudicating officer appointed under subsection (1) of Section 46.
Affixing Digital Signature	With its grammatical variations and cognate expressions, means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
Appropriate Government	It means as respects any matter- (i) Enumerated in List II of the Seventh Schedule to the constitution (ii) Relating to any State law enacted under List III of the Seventh Schedule to the constitution, the State Government and in any other case, the Central Government.
Asymmetric crypto system	It 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.
Certifying Officer	A person who can be granted a licence to issue a Digital Signature certificate under Section 24

Certification Practice certificate	It means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates
Computer	It means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulation of electronic, magnetic or optical impulses. It includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.
Computer Network	It means the interconnection of one or more computers through- (i) The use of satellite, microwave, terrestrial line or other communication media, and (ii) Terminals or a complex consisting of two or more interconnected computer whether or not the interconnection is continuously maintained.
Computer Recourse	It means computer, computer system, computer network, data, computer data base or software.
Computer system	It means a device or collection of devices, including input and output support devices. It excludes calculators which are not programmable and capable or being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that perform logic, arithmetic, data storage and retrieval, communication control and other function.
Controller	It means the Controller of Certifying Authorities appointed under sub-section (1) of Section 17
Cyber Appellant Tribunal	It means the Cyber Regulation Appellant Tribunal established under sub-section (1) of Section 48.
Data	It means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network. It may

	be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory or the computer.
Digital Signature Certificate	It means a digital signature certificate issued under sub-section (4) of Section 35
Electronic Form	Electronic form, with reference to information, means any information generated, sent, received or stored in media, magnetic, optical computer memory, micro film, computer generated micro fiche or similar device.
Electronic Gazette	It means the Official Gazette published in the electronic form
Electronic record	It means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro filche.
Function	In relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer
Information	It includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer-generated micro fiche.
Intermediary	With respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message
Key Pair	It is an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by private key.
Originator	It means a person, who sends, generates stores or transmits any electronic message, or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.
Private Key	It means the key of a key pair used to create a digital signature.

Public Key	It means the key of a key pair used to verify a digital signature and listed in the digital signature certificate.
Secure system	It means computer hardware, software and procedure that- (a) Are reasonably secure from unauthorised access and misuse, (b) Provide a reasonable level of reliability and correct operation, (c) Are reasonably suited to performing the intended functions, and (d) Adhere to generally accepted security procedures.
Subscriber	Subscriber means a person in whose name the digital signature certificate is issued.
Verify	To verify, in relation to a digital signature, electronic record or public key, means to determine whether- (a) The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber (b) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

DIGITAL SIGNATURE

Section 2(1)(p) defines digital signature, "mean authentication of any electronic record by a subscriber by means ofan electronic method or procedure in accordance with the provisions of Section 3".

Authentication is a process used to confirm the identity of a person or to prove the integrity of information. Messages authentication involves determining the source and verifying that it has not been modified or replaced in transit.

LIKH LE PAAPI....

SECURE DIGITAL SIGNATURE

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 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.

ELECTRONIC RECORD AND E GOVERNANCE

1. ***Legal recognition of Electronic Records (Section 4)***

   Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then 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 used for a subsequent reference.

LIKH LE PAAPI....

2. ***Legal recognition of digital signatures (Section 5)***

   Where any law provides that information shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature.

LIKH LE PAAPI....

3. ***Use of electronic records and digital signatures in Government and its agencies***

Where any law provides for the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government or the issue or grant of any license, permit, sanction or approval or the receipt or payment of money, then such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, is effected by means of such electronic form as may be prescribed by the appropriate Government.

LIKH LE PAAPI....

4. ***Retention of electronic records***

(1) 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, if -

(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 dispatch or receipt of such electronic record are available in the electronic record;

LIKH LE PAAPI....

5. ***Publication of rules, regulations, etc., in Electronic Gazette***

Where any law provides that any rule, regulation, order, by-laws, 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:

LIKH LE PAAPI....

6. ***Section 6,7 and 8 not to confer right to insist document should be accepted in Electronic form***

Nothing contained in Section 6,7 and 8 shall 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 electronic form.

LIKH LE PAAPI....

7. ***Power to make rules by Central Government in respect of digital signature***

The Central Government may, for the purposes of this Act, by rules, prescribe -

(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.

DATA PROTECTION

As per Section 43A of the Information technology Act, 2000, where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, ***not exceeding five crore rupees***, to the person so affected.

SCOPE OF CYBER LAWS

E-commerce Law

E-commerce defined as the commercial transaction of services in an electronic format. It is also referred to as "any transaction conducted over the Internet or through Internet access, comprising the sale, lease, license, offer or delivery of property, goods, services or information, whether or not for consideration, and includes the provision of Internet access". The US Census Bureau measures e-commerce by looking at "the value of goods and services sold online whether over open networks such as the Internet, or over proprietary networks running systems such as EDI.

LIKH LE PAAPI....

Online Contracts

An online contract follows the same pre-requisite as being followed in offline (physical) contract. At a basic level, online contract formation requires online offer/proposal by one party and its online acceptance by the other party. Electronic contracts, by their very nature, are dynamic and often multi layered transactions. With a layered contract, agreement to a contract may not occur at a single point in time.

LIKH LE PAAPI....

Business Software Patenting

Patent protects a process, while copyright protects expression. Patents confer stronger rights than copyrights. One computer programme consists of thousands of instructions. Every programme is unique, as it is a combination of logically arranged algorithms and techniques. Programmes are covered under copyright law, whereas, algorithms and techniques qualify for patenting.

With the advent of worldwide web and e-commerce coming of age, the debate of software patenting acquired a new platform in the form of 'business software patents'.Big e-commerce etailers, like Amazon, Priceline and EBay are going for patenting the backend software technologies of their front-end operations.

LIKH LE PAAPI....

E taxation

Ecommerce is considered by many national tax administrations not only as having the potential for creating a new stream of revenues but also as presenting daunting challenges to national tax systems because new technologies used for E-Commerce open up probabilities of tax evasion and avoidance.

In order to properly tax commercial transactions, it is critical to establish the systems by which the tax authorities can obtain accurate and necessary information on those transactions, regarding transacting parties, time, place and volume. Even though many scholars believe that existing domestic and international tax regulations may well fit E-Commerce, nonetheless, this new type of commercial transaction raises the need of modification and adjustment of these existing regulations because of the born-global nature of E-Commerce.

LIKH LE PAAPI....

E-governance

The World Bank defines e-governance as the use of information and communication technologies by government agencies to transform relations with citizens, business and other arms of the government.

It involves information technology enabled initiatives that are used for improving (i) the interaction between government and citizens or government and businesses - e-services (ii) the internal government operations - e-administration and (iii) external interactions - e-society.

Cyber laws facilitate e-governance practices by promoting various e governance initiatives, like electronic filing of documents with the Government agencies, use of electronic records and digital signatures in Government and its agencies, retention or preservation of electronic records in electronic form and publication of rule, regulation, etc., in Electronic Gazette.

LIKH LE PAAPI....

CYBER CRIMES

Intentional use of information technology by cyber terrorist for producing destructive and harmful effects to tangible and intangible property of others is called Cyber Crime. Cyber-crime is an issue which has no national boundaries. Cyber Crime is generally used to describe criminal activity in which computer or/and network is a tool, a target, or a place of criminal activity. It generally includes traditional crimes in which computer or networks are instrumental to commit them. Some authors use computer crime and cyber-crime as interchangeable terms, signifying that the two are same. Some definitions of computer crime are listed below.

1. Marc M Goodman says that a computer crime can be classified into three categories
   - As crime where computer is target
   - Crimes where computer is the tool of the crime
   - Crimes where computer is instrumental

2. Nandan Kamat says that since the internet is composed of computers, crimes occurring on the internet are computer crimes. He also says that a computer can be subject of a crime by being stolen or damaged, it can be the site of crime such as fraud or copyright infringement, or it can be the instrument of a crime such as when it is used to access other machines or store information illegally.

3. Suresh T Vishwanathan defines computer crime as (i) any illegal action in which a computer is a tool or object of the crime, in other words, any crime, the means or purpose of which is to influence the purpose of computer (ii) any incident associated with computer technology in which a perpetrator by intention made or could have made a gain and (iii) computer abuse is considered as any illegal, unethical or unauthorised behaviour relating to the automatic processing and transmission of data.

Some other authors argue that when a crime is committed to or by a computer using the internet, it is just a computer crime. According to them a cybercrime can be understood as one, which is committed with the help of internet, abusing the special characteristics of internet, anonymity, absence of geographic boundaries.

Cyber Crime is promoted by the various factors like new technologies, complexity and loss of evidence. The computers are easy to access by means of these new complex technologies. The unauthorised access to a computer system is made possible by installing technologies like key loggers that can steal the access codes, voice recorders etc. that can bypass firewalls and get into the system.

CLASSIFICATION OF CYBER CRIME

Cyber Crime can be classified on various basis such as on the basis of:

(a) subject of crime,

(b) against whom crime is committed and

(c) on the basis of temporal nature of criminal activities being carried out on computers and internet.

The subject of cybercrime may be broadly classified under the following three groups:

Against individuals

It may be committed against individual person or property. Following are some crimes that can be committed against an individual:

1. Harassment via e-mail
2. Cyber-stalking
3. Dissemination of obscene material
4. Defamation
5. Unauthorised control/ access over computer system
6. Indecent exposure
7. Email spoofing
8. Cheating and fraud

Following are the crimes which can be committed against individual property.

1. Computer vandalism
2. Transmitting virus
3. Netrespass
4. Intellectual Property crimes
5. Internet time thefts

Against organisation

Following are the crimes that can be committed against organisations.

1. Possession of unauthorised information
2. Cyber terrorism against the government organisation
3. Distribution of pirated software

Against society

1. Polluting the youth through indecent exposure
2. Trafficking
3. Financial crimes
4. Sale of illegal articles
5. Online gambling
6. Forgery

The above list is not exhaustive. In addition to above listed crimes, crimes such as hacking, denial-of- service attack, malicious crime (including use of virus), e-mail bombing, salami attacks, data didling, web jacking, etc. find place in cyber space.

Recently users of Facebook have been targeted by hackers and cybercriminals attempting to access their user profiles and steal valuable data. Facebook allows people to develop and write games and software to run on the site, but these applications do not need to be approved by Facebook before they are made available for people to download. High-tech thieves have started to take advantage of this loophole to create fake applications that contain malicious software. Koobface virus, a worm, works by prompting Facebook users to visit a fake YouTube page, and then installs malicious software on their computers. The worm then burrows into the computer's operating system, and hunts for cookies; the digital record of websites visited and uses this information to log into other social networks the user may be member of.

Me – Sir Module kholna padega??

Vikas Sir – Of course, paapiyo, Module sab kuch hai. Penalty padho ab module se....

REGULATION OF CERTIFYING AUTHORITIES

APPOINTMENT OF CONTROLLER AND OTHER OFFICERS (SECTION 17)

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

(2) The Controller shall discharge his functions 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 by the Central Government.

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

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

LIKH LE PAAPI....

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 interests 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.

LIKH LE PAAPI....

Recognition of Foreign Certifying Authority

(1) 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.

(2) Where any Certifying Authority is recognized, the Digital Signature Certificate issued by such Certifying Authority shall be valid.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition, he may, by notification in the Official Gazette, revoke such recognition.

LIKH LE PAAPI....

Controller to act as repository

(1) The Controller shall be the repository of all Digital Signature Certificates.

(2) The Controller shall make use of hardware, software and procedures that are secure intrusion and misuses or observe such other standards by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerized data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

LIKH LE PAAPI....

License to issue Digital Signature Certificates

(1) Any person may make an application, to the Controller, for a license to issue Digital Signature Certificates.

(2) No License shall be issued, unless the applicant fulfills requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates.

(3) A license granted under this section shall -

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

(b) not be transferable or heritable;

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

LIKH LE PAAPI....

Power to investigate contraventions

(1) The Controller or any Officer authorized by him shall take up for investigation any contravention.

(2) The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities.

LIKH LE PAAPI....

BY ADJUDICATING OFFICER

Power to adjudicate

(1) For the purpose of adjudging whether any person has committed a contravention, Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent 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.

(2) The adjudicating officer shall, after giving the person 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.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience.

(4) 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.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal and all proceedings before it shall be deemed to be judicial proceedings under the Indian Penal Code or shall be deemed to be a civil court under Code of Criminal Procedure, 1973.

LIKH LE PAAPI....

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.

LIKH LE PAAPI....

Non compliance with the directions of the Controller

- The Controller is empowered to direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities if those are necessary to ensure compliance.
- Any person who fails to comply with any such order shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.
- Further, under section 69 of the Act, the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, if satisfied that it is necessary or expedient so to do 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 commission of any cognizable offence, may, for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource and the subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency, which has been so directed, extend all facilities and technical assistance to provide access to such computer resource or intercept, monitor or decrypt the information, as the case may be.

- The subscriber or intermediary or any person who fails to assist the agency referred to above shall be punished with an imprisonment for a term, which may extend to seven years and shall also be liable to fine.
- Likewise, sections 69A and 69B have been incorporated to block for access by the public any information generated, transmitted, received, stored or hosted in any computer resource and to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource respectively.

LIKH LE PAAPI....

CYBER APPELLANT TRIBUNAL

The Act provides for the establishment of the Cyber Appellate Tribunal. Its establishment, composition, Jurisdiction, powers, procedures is as follows:

Establishment of Cyber Appellate Tribunal

(1) The Central Government shall establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Composition of Cyber Appellant Tribunal

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.

LIKH LE PAAPI....

Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal

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,

(b) Is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that service for at least three years.

Term of Office

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.

Filling up of vacancies

If any vacancy occurs in the office and the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person to fill the vacancy and the proceedings may be continued before the Cyber appellate Tribunal from the stage at which the vacancy is filled.

Resignation and Removal

(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office provided that the said Presiding Officer shall relinquish his office 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.

(2) The Presiding Officer of a Cyber appellate Tribunal shall not be removed from his office on the ground of proved misbehavior or incapacity after an inquiry made by a judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may regulate the procedure for the investigation of misbehavior or incapacity of the Presiding Officer.

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

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

Appeal to Cyber Appellate Tribunal

(1) Any person aggrieved by an order made by Controller or an adjudicating officer may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal shall be filed within a period of twenty 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 provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of twenty five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) 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.

(5) 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.

(6) The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as quickly as possible and efforts shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

LIKH LE PAAPI....

Procedure and powers of the Cyber Appellate Tribunal

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of civil Procedure, 1908 but shall be guided by the principles of natural justice and the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, 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.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding and the Cyber Appellate Tribunal shall be deemed to be a civil court under CPC.

Right to Legal Representation

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

Limitation

The provisions of the Limitation Act 1963, shall, as far as may be, apply to an appeal made to the cyber appellate tribunal.

Civil court not to have jurisdiction

No Court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer or the Cyber Appellate Tribunal is empowered under this Act to determine and no injunction shall be granted by any court or any other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this 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. Provided that the High Court may, allow it to be filed within a further period not exceeding sixty days.

Compounding of contraventions

(1) Any contravention 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, subject to such conditions as the controller or such other officer or the adjudicating officer may specify.

(2) Nothing shall 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.

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

Recovery of Penalty

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrears of land revenue and the license or the digital signature certificate, as the case may be, shall be suspended till the penalty is paid.

Confiscation

Confiscation of computers or any accessories provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act has been or is being contravened.

Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate offences under this Act

Immunity to network service providers in certain cases

Act immunizes the network service provides i.e., an intermediary from liability under this Act, rules or regulations made thereunder for any third party information, data, or communication link made available or hosted by him if

(a) His function is limited to providing access to a communication system,
(b) He does not initiate the transmission, select the receiver or select (or modify) the information, and
(c) Observes due diligence while discharging his duties.

Further, the new amendments have introduced section 79A for the purposes of providing expert opinion on electronic form evidence, i.e., the Central Government to notify examiner of electronic evidence.

Power of Police officer and other officers to enter, search etc

Act provides that any police officer not below the rank of an Inspector, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act.

The provisions authorized to carry out search and arrest only in public place includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

Under this provision, the Central Government has got the power to authorize any other officer, other than police officer, to carry out search and arrest. If a person is arrested by such other officers, the arrested person has to be produced before the Magistrate having jurisdiction in the case or before the officer-in charge of a police station without unnecessary delay.

LIKH LE PAAPI....

CYBER REGULATIONS ADVISORY COMMITTEE (CRAC)

Section 88 of the Act provides for the constitution of CRAC. The CRAC 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 subject-matter as the Central Government may deem fit.

The non-official members shall be paid such traveling and other allowances as the Central Government may deem fit. The CRAC shall advice:

(a) The Central Government either generally as regards any rules or for any other purpose connected with this Act;

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

Section 89 of the Act authorized the Controller to make, after consultation with the CRAC and with the previous approval of the Central Government, regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act. Such regulations may provide for all or any the following:

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority;

(b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority;

(c) the terms and conditions subject to which a license may be granted;

(d) other standards to be observed by a Certifying Authority;

(e) the manner in which the Certifying Authority shall disclose the matters;

(f) the particulars of statement which shall accompany an application;

(g) the manner by which the subscriber communicate the compromise of private key to the certifying authority.