Vidyasagar College of Arts and Science
Approved by UGC, Affiliated to Bharathiar University & Re-Accredited by NAAC
Udumalpet - 642122

NH83Udumalpet–PollachiRoad,Udumalpet–642122 Cell : 98430 24997, 97877 21960
e-mail : vcasudt@yahoo.comwebsite:www.vidyasagarcollege.org

Course: B.Com(PA) Batch : 2023-26 Semester:VI

SUBJECT : CYBER LAW

CYBER LAW

Basic Knolwedge of Cyber Law

UNIT I **CYBER LAW**

Cyber Law: Introduction- concept of cyber space - E-Commerce in India - Privacy factors in E-Commerce - Cyber law in E-Commerce- Contract Aspets.

UNIT -II **SECURITY ASPECTS**

Security Aspects : Introduction- Technical Aspects of Encryption-Digital Signature - Data Security - Intellectual Proprty Aspects: WIPO-GII- ECMS-Indiancopyrights act on Soft Propriety Works- Indian Patents Act on Soft Propriety Works.

UNIT -III **EVIDENCE ASPECTS**

Evidence Aspects : Evidence as Part of the Law of Procedure - Applicability of the law of Evidence on Electronic Records - The Indian Evidence Act 1872 - Criminal Aspect : Computer Crime - Factors Influencing Computer Crime- Strategy for Prevention of Computer Crime.

UNIT -IV **GLOBAL TRENDS**

Global Trends : Legal ramework for Electronic Data Interchange: EDI Mechanism- Electronic Data Interchange Scenario in India.

UNIT - V THE INFORMATION TECHNOLOGY ACT 2000

The INformation Technology Act 2000- Definitions - Authentication of Electronic Records- Electronic Governance - Digital Signature Certificates.

Reference:

The Indian Cyber Law : Suresh T.Viswanathan, Bharat Law House, New Delhi.

Cyber Law ;

Net Sources.

- **CONCEPT OF CYBER LAW AND CYBER SPACE**

1.2 Cyber Law - meaning

Cyber law is the law which regulates the operations performed by the user via network by electronic means.

In other words, we can say cyber law regulates the cyber space Cyber Law.

1.3 Features of Cyber Law

Cyber law contains the following features:

1. It contains a set of rules and guidelines.
2. It defines the legal internet activities.
3. It specifies the illegal activities which are punishable under law.
4. It provides legal framework for all the activities which are carried out through the network.

1.4 Significance of Cyber Law

Now, we are relying upon information technology to carry out various day to day operations. Information technology has varied applicability in almost all aspects of our life. Some of the areas are science and engineering, business, education and entertainment. Though we are utilizing information technology frequently in some of the areas, we have to be equally cautious. For example, due to the anonymous nature of the Internet, it is possible for the fraudulent people to

involve in a variety of criminal activities. Some of the criminal activities are

1. Launching of malicious software in the form of worms, viruses, trojans, spyware, adware, etc.,
2. Computer hacker tries to break into computer system, especially to get secret information.
3. Downloading unauthorized software.
4. Selling illegal articles such as narcotics, weapons, etc.,
5. Gaming activities through online.
6. Stealing of money from banks using networks.
7. Credit card frauds.
8. Cyber stalking, cyber defamation, indecent & abusive mails.
9. Stealing the business secrets and documents.
10. Stealing of data in BPO centers.
11. Stating false advertisements in the web page, e-mail and sms.

To overcome the above said criminal activities, various security measures are applied. Still, lots of cyber crimes are going on. So, there is a need for cyber law.

1.7 Cyber Space-meaning

Cyber space is a domain characterized by the use of electronic and electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure.

1.8 Inclusive of Cyber Space

- Computer
- Mobile phone
- idual,

- ATM
- Data storage device
- Software
- Network
- Website
- E-mail

1.9 Facilitating functions of cyber space

- e-business
- e-banking
- e-shopping
- cal For
- e-receipts & payments
- e-transmission of the documents
- e-education
- e-medicine
- e-information
- e-database
- e-entertainment
- e-engineering

1.10 Major issues in cyber space

The following are the major issues related to cyber space:

(1) Developments of cyber space pave the way for cyber crimes.

(2) In some cases, identification of the user is not possible.

(3) E-mail address has digital identity, but it does not show the reliable identity.

(4) Passwords are used as identity but are shared easily.

(5) Internet protocol (IP) addresses serve as an address for a computer. But it does not identify the user of a computer.

- **E COMMERCE**

2.1 E-commerce - meaning

E-commerce is otherwise known as Electronic commerce. The activities involved in buying and selling of products or services over the internet through an electronic medium are termed as E-commerce.

2.2 History of E-Commerce

1. 1970s: Electronic Funds Transfer (EFT)
   - ◆ Used by the banking industry to exchange account information over secured networks.
2. Late 1970s and early 1980s: Electronic Data Interchange (EDI) used in e-commerce within companies.
   - ◆ Used by businesses to transmit data from one business to another.
3. 1990s: the World Wide Web on the Internet provides easy-to-use technology for publishing and disseminating information.
   - Cheaper to do business (economies of scale).
   - Enable diverse business activities (economies of scope)

2.3 Divisions of Electronic Commerce

Depending upon parties involved, E-commerce can be classified into four major

categories.

1. Business to Business (B2B)

Business to Business e-commerce is an industrial marketing strategy which is done through online process. E-distributors, supply products and services directly to many individual businesses. The buyers can quickly search for the suppliers' information; can place an order and make the payment through electronic payment mode. This process is done via internet.

Examples of Business to Business websites

http://www.eurotradenet.com

http://www.thesourceengine.co.uk

http://www.eindiabusiness.com

http://www.ec21.com

2. Business to Consumer (B2C)

The business to consumer model of e-commerce involves selling of products and services by a company to individual consumers over internet. B2C involves electronic retailing or e-tailing which enables the manufacturer to conduct online retail

sales and sell directly to the consumer. Consumer can access the internet at any time, order goods/services and can make payment through electronic payment mode.

sales and sell directly to the consumer. Consumer can access the internet at any time, order goods/services and can make payment through electronic payment mode.

Examples of Business to consumer websites

http://www.amazon.com/

http://www.dell.com/

3. Business to Government (B2G)

B2G is defined as the business between the companies and public enterprises. It involves the use of internet for public procurement, licensing procedures and for other government related

operations.

4. Consumer to Consumer (C2C)

C2C e-commerce involves transactions between consumers. In this mode, a consumer posts an item for rate on a website offered by a third party (e-bay) who facilitates the seller for selling the goods by charging a fees or commission. The consumer bid to purchase it.

Examples of consumer to consumer websites

http://www.ebay.in/

http://www.flipkart.com/

http://www.futurebazaar.com/

http://www.indiaplaza.com/

2.4 Benefits of E-Commerce

The following are the benefits of e-commerce:

(i) Provides huge publicity of product/service to the millions of visitors on the web.

(ii) The people can visit the online store at the convenient time.

(iii) Cost is effective when compared to traditional methods.

(iv) It is possible to compare the similar product at a time.

(v) It provides abundant information across product lines.

(vi) It creates market for niche products.

(vii) It is an aid for the people to make e-payments and to apply Electronic Data Interchange (EDI).

2.6 E-commerce in India

E-Commerce, propelled and diffused by IT, has come up as an important driving force of economic development. Increasing IT diffusion strengthens and enlarges the scope of E-commerce. Government of India has taken corrective measures to strengthen the infrastructure

for a healthy growth of e-commerce. Appropriate rules and regulations are being implemented for safe and secure transactions on the internet. E-commerce is one of the most successful by-product of the internet revolution and India isn't far behind. According to the report entitled 'Online and Upcoming: The Internet's Impact on India', Internet generated 1.6 percent of the GDP or about $30 billion in 2011. This could grow to 2.8 to 3.3 percent by 2015, if India achieves its potential for growth in the number of Internet users and Internet technology-related consumption and investment stated by McKinsey & Company partner, Chandra Gnasambandam. And further he stated that, it facilitated about six million direct and indirect jobs in 2011. This could grow to 22 million by 2015. if India follows an inclusive path of Internet expansion. India with a user base of 120 million users.

Source :

India is the world's third largest Internet market is poised to garner up user base with 480 million users, followed by US (245 million) in to 370 million users in 2015. China has the world's largest Interne 2011. By 2015, China is expected to have 583 million users, while the US is expected to have 279 million users.

Source:

http://profit.ndtv.com/news/economy/article-internet-to contribute-100-billion-to-ndias-gdp-by-2015-mckinsey-314970

2.7 Privacy factors in e-commerce

Privacy is said to be the control over one's personal data against disturbance from others. Lack of security and the attempted access to data in an unauthorized way are two critical problems for consumers, e-business, and government.

Consumer privacy

Privacy as a consumer issue is extremely sensitive in the surrounding context. To deliver the products/services, business people collect personal information from the customers. Sometimes on request from others, they may be sharing this information with them. Apart from this, fraudulent people intrude on web pages to collect personal information of the customers who are involved in online shopping. By observing the web page, we can know their intrusive

approaches such as data requests through pop-up windows.

Currently, many business people develop and disclose a privacy policy statement in their websites. They expect that, reading such privacy policy statement can reduce customer's perceived privacy risks associated with the disclosure of their personal information.

Various regulations have been enacted to protect an individual's privacy across countries, Some of them are, Health Insurance Portability and Accountability Act (US), Personal Information Protection Electronic Document Act (Canada) and Data Protection Directive (EU), Information Technology Act (India).

Business Privacy

A major hurdle for the growth of e-business all over the world is the privacy of online data, Internet provides greater access to data not only to legitimate users, but also to hackers and corporate spies. Business strategies and secrets are stolen from the websites, Competitors make use of this as a competitive advantage. E-commerce sites fear financial losses and bad publicity.

So it is necessary to enhance current security measures to protect their information.

28 Cyber law in E-commerce

In the present globalised scenario, e-commerce is not a new phenomenon. In the recent years, e-commerce has grown tremendously with new technologies and innovations.India has made some progress in legalizing the electronic contracts format and electronic transactions through authentication of the electronic documents and records. On the other hand, to prevent misuse of the Internet in e-commerce, there are some Indian laws to tackle cyber crime with stipulated punishment in the form of imprisonment and fines.

India enacted the first Information Technology Act, 2000 recommended by the general assembly of the United Nations by a resolution dated 30 Jan. 1997. Following the UN resolution, India passed the Information Technology Act 2000 in May 2000 and notified it for effectiveness on October 17, 2000. The Information Technology Act 2000 has been substantially amended through the Information Technology (Amendment) Act 2008 which was passed by the two Houses of the Indian Parliament on December 23 and 24, 2008, It got the Presidential assent on February 5, 2009 and was notified for effectiveness on October 27, 2009.

It provides legal framework for transactions carried out by means of electronic data interchange and other means of electronic communication. Still strong legal back up is required to support all types of 'virtual' contracts and as well as transactions between parties. There must be national laws, in tandem with international laws and conventions, to boost up e-commerce.

2.9 Contract

A voluntary and legally binding agreement between two or more competent parties is said to be a contract. According to Section 10, The Indian Contract Act, 1872, defines the term "Contract' as "All agreements are contracts, if they are made by the free consent of the parties, competent to contract, for a lawful consideration with a lawful object, and not hereby expressly to be void."

Business communication and relationships have changed with the emergence of various communicative applications. The environment where the contract is taking place has also changed. Traditional contracts took place with the two sides having a face to face consultation, whereas electronic contract takes place in the virtual space wherein the two companies would not even meet each other. The rapid growth of the internet as a tool for commerce has brought a rapid shifting of common transactions from the market place to space.

Categories of online Contract

Contracts formed over the internet usually fall into 3 broad categories

1. Contract for the sale of goods.
2. Contract for the supply of digitized products.
3. Contract for the supply of services and facilities.

2.10 Essentials of online contract

The following should be addressed in online contracts:

1. Contract formation

The contract terms should state the method and procedure for accepting the offer, as well as the duration of the offer and any conditions relating to it.

2. Delivery

The method and timing of delivery of the relevant goods should be specified.

3. Risk and Insurance

Where physical goods are to be dispatched, the question of risk of damage or loss and the responsibility for insurance should be stated.

4. Price, Currency and Payment

The contract should state the price clearly (including any applicable taxes and insurance), the currency acceptable and means of payment.

5. Authenticity

To make electronic document as genuine, digital signature is necessary. It is essential in helping to promote e-commerce because it ensures that all parties have entered in a binding contractual agreement. It is an evidence to integrate the electronic contract.

6. Confidentiality

Confidentiality is concerned with the privacy of information. Customers may not want to share their personal information to others and also the suppliers may not be interested to show special rates being quoted to a particular group. Most of them may be maintaining the confidential information in the electronic storage. So, it is necessary to ensure proper security measures to enhance the confidentiality.

7. Integrity

Message sent via internet can be altered while passing through many routing stations and packet-switching nodes. When the persons distribute documents electronically, it is often important to note that the content has not been altered. Both the persons should confirm whether the message sent and received are identical.

8. Non repudiation

It may possible for the signatory to deny the signatory document. Non-repudiation is a document security service that prevents the signor of the document from denying the signatory

document.

UNIT - II

3. DATA SECURITY

3.1 Data security-meaning

In any electronic transactions data security is a must. Data Security means protection of database from hackers by using security measures. Unauthorized access of data or destruction of data may lead to numerous problems for larger corporations and also for the personal home users. Data security is an important area of concern for every business owner, consumer and for the individual also for the personal home users. Data security is an important area of concern for every business owner, consumer and for the individual.

3.4 Encryption -meaning

Encryption is a process of translating a message, called the Plaintext, into an encoded message, called as Cipher text. Plaintext is an unencrypted message, before it is passed through an Encryption algorithm (Cipher). A Cipher is a computer software algorithm which is used for Encryption.

With the Encryption, the data can be securely transmitted via the Internet. Encryption can protect the data at the simplest level by preventing other people from reading the data. The data that they see appears to be gibberish without a way to decode it.

3.5 Advantages of Encryption technology

Encryption technologies can help in the following ways:

- It establishes the identity of users.
- It controls the unauthorized transmission or forwarding of data.
- Receiver can verify the integrity of the data. (i.e., that it has not been altered in any way)
- It ensures that users take responsibility for data that they have transmitted.
- It helps to keep communication secret.

- **Means of encryption of data**

The encryption of data involves

1. Symmetric encryption
2. Public Key Encryption, or asymmetric encryption

1. Symmetric encryption

The basic means of encryption of data involves a symmetric encryption. Here a key is used to encrypt and also to decrypt data. For example-if the sender and receiver uses a computer to generate a random match-up of the 26 letters with 26 numbers according to a scheme where 6 = A, 13=B, 2 = C, etc. and thus it can be encoded and decoded by matching up the same scheme(Key). These codes are fairly easy to crack by hackers. Even, much more complex codes generated by algorithms, can also be broken by powerful computers when only one key exists.

2. Public Key Encryption or asymmetric encryption

Public Key Encryption, or asymmetric encryption, is much more important than symmetric encryption in e-commerce. The big improvement brought by Public Key Encryption was the introduction of the second key which makes a difference in terms of protecting the integrity of data.

Asymmetric Encryption is a form of encryption where keys come in pairs. One key encrypts, only the other can decrypt.

Public Key Encryption relies on two keys,

(a) Public key and

(b) Private key

(a) Public Key

A Public Key is a publically distributed key, used in Asymmetric Encryption. It is mathematically equivalent to a Private Key. Public Key's are frequently certified by a Certificate Authority, so that users of this key can verify its authenticity. A Certificate Authority is a trusted third party, which certifies Public Key to their claimed owners.

(b) Private Key

If you have public key, you cannot infer the other key.

For example, if you send encoded message via network to another person by giving the public key to the user, the user who sees the message cannot read it, because he has only the public key. The message only makes sense when the user has the copy of the private key, which does the decoding magic, to turn the zeros and ones (bits of information) into readable text.

Since users typically create a matching key pair, they make one public while keeping the other secret. Users can "sign" messages by encrypting them with their private keys. This is effective since any message recipient can verify that the user's public key can decrypt the message, and thus prove that the user' secret key was used to encrypt it.

Users can send secret messages by encrypting a message with the recipient's public key. In this case, only the intended recipient can decrypt the message, since only that user should have acces to the required secret key.

Public Key Encryption ostensibly creates a world in which it does not matter if the physical network is insecure. Even if - as in the case of a distributed network like the Internet, where the data passes through many hands, in the form of routers and switches and hubs-information could be captured, the encryption scheme keeps the data in a meaningless form, unless the cracker has the private key.

3.7 Public Key Infrastructure

Public Key Infrastructure (PKI) is a system which is established to have a secured communication over network.

It consists of

- Set of servers,
- Software,
- Protocols and
- Application programs used to manage the Private Keys and Public Keys of a group of users.

The PKI would create an environment where any Internet user could "carry" certificates to identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seam-less and robust PKI would have enormous implications for speed-ing the growth of e-commerce.

3.9 Digital signature

A Digital Signature Certificate (DSC), like handwritten signature, establishes the identity of the sender while filing the documents through internet which a sender cannot revoke or deny. Digital Signature Certificates (DSC) are the digital equivalent (that is, electronic format) of physical or paper certificates.

Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as a proof of identity of an individual for a certain purpose; for example a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove the identity, to access information or services on the Internet or to sign certain documents digitally.

3.10 Features of digital signature certificate

The following are some of the features of digital signature certificate:

- It helps to sign certain documents digitally.
- It ensures that no alterations are made to the data once the document has been digitally signed.
- It is normally valid for 1 or 2 years, after which it can be renewed.
- It is a method of verifying the authenticity of an electronic document.
- The IT Act has given legal recognition to digital signature meaning, that is, legally it has the same value as handwritten or signed signatures affixed to a document for its verification.
- It is accepted for Northern Railway, MCA 21, E-filing, E-tendering etc...

3.14 Types of Digital Signature

There are 3 types of Digital Signature Certificates, having different security levels, namely: - Class-1, Class-2, Class-3. Each has its own level of security and is meant for a particular category of professional and or sector of industry.

Class-1

Class-1Digital Signature Certificates facilitates the individuals to send the message through email by affixing digital signature. Here, no personal verification is done by the certifying authority while issuing the digital signature certificate. So the legal validity of the certificate is limited.

Class-2

Class-2 Certificates are issued to Individuals, Government Organizations and Devices. Individual Certificates are appropriate for digital signatures, encryption, and electronic access control. Device Certificates are appropriate for device authentication; message, software, and content integrity; and confidentiality encryption.

Eg.. Authentication for following softwares in a computer systems along with internet access.

#Windows 2000/Windows XP

#Internet Explorer 6.0

#Adobe Acrobat Reader 7.0.5

#Java Runtime Environment (JRE)

Class 2 A Digital Signature Certificate is issued to individuals as a personal certificate that provides second highest level of assurance.

These are mainly used to file the Income Tax Returns, to file the documents with ROC (Registrar of companies) and Ministry of Corporate Affairs. These are also used by Chartered Accountants and Company Secretaries for their clients. Here, the identity of a person is verified against a trusted, pre-verified database by a certifying authority.

Class 3

Class 3 Digital Signature Certificates are used for e-Tendering / e-Procurement/ e-Bidding/e-Ticketing /e-Auction/e-Bidding. Typically, they are used for electronic data exchange, internet banking/broking-tendering and other web-based transactions where confidentiality and authenticity are critical.

Class 3a Individual certificates are issued to individuals or devices and encompass primarily high end security-sensitive online activity.

Class 3b Organization certificates are those which are used for signatures, encryption, electronic access control, e-commerce, and online financial transactions that require a strong assertion of the customer's identity.

This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/her identity to get the digital signature certificate.

Example

CERTIFYING AUTHORITY

TCS-CA is a licensed Certifying Authority (CA) and is authorized by the Controller of Certifying Authorities (CCA), Government of India, to issue legally valid Digital Certificates in India under the Indian IT Act 2000.

Tata Consultancy Services-Certifying Authority (TCS-CA) offers a range of Digital Certificates for multiple applications. Depending on the level of trustworthiness, TCS-CA offers three classes of Personal Certificates:

- Class-1
- Class-2

- Class-3

3.15 Components of a Digital Signature Certificate

- Public key: any one can get a copy of this and is part of the verification system.
- Name and e-mail address: enables the viewer to identify the details.
- Expiry date of the public key: used to set a shelf life.

4. Name of the company: identifies the company that the sture belongs too.
5. Serial number of the Digital ID: unique number that is bundled to the signature for tracking extra identification reasons.
6. Digital signature of the CA (Certification Authority): signed by the authority while issuing the certificates.

3.16 lise of Digital Signature Certificate

1. It can be used to access secured zones of web sites where member login is required, surpassing the requirement of entering the user name and password.

2. It ensures by means of verification and validation that the user is whom he/she claims to be.

3. This is done by combining the users credential to the digital certificate and in turn this method uses one point of authentication.

4. Digital certificates ensure confidentiality and ensure that messages can only be read by authorized intended recipients.

5. Digital certificates also verify date and time so that senders or recipients cannot dispute if the message was actually sent or received.

6. Used to sign digitally in e-mails which can be sent through Outlook Express/MS-Outlook etc.

7. It enables the e mail receiver to ensure that the mail has come from correct person only.

3.17 Professionals who require Digital Signature Certificate

Under MCA21, all the authorized signatories of compa and professionals who sign the

manual documents are required obtain a Digital Signature Certificate (DSC). Therefore following personnel have to procure Digital Signature Certificate:

1. Directors
2. CA's/Auditors
3. Company Secretary - Whether in practice or in job
4. Bank Officials - for Registration and Satisfaction of Charges
5. Other Authorized Signatories

3.18 Credentials required with Application Form

- Proof of identity
- a self attested copy of PAN Card
- Valid Active PAN with the Income Tax Department
- Proof of residence – Anyone
- a self attested copy of latest bill: WATER ELECTRICITY/POWER/TELEPHONE / CREDIT CARD or VOTER'S ID CARD / DRIVING LICENSE PASSPORT in the applicant's name for address confirmation

- **INTELLECTUAL PROPERTY ASPECTS.**

4.1 Intellectual Property Rights

Intellectual Property Rights (IPR) are important aspect of Cyber laws. IPR refers to the right over the ownership of intellectual property.

It is broadly divided into two categories:

I. Copyright

Copyright can be made for literary and artistic works such as novels, poems and plays, films, musical works, drawings, paintings, computer programs, photographs, sculptures, and

architectural designs.

II. Industrial property

It includes inventions (patents), trademarks, industrial design and geographic indications of source. Geographical indication in used to identify goods having special characteristics originating from a definite territory.

a. Patent

A patent is a set of exclusive rights granted by the government to an inventor or their assignee for a limited period of time (usually 14 years), in exchange for the public disclosure of the invention. A patent protects a new inventions, discoveries and designs.

b. Trade marks

A Trademark is an exclusive right granted for distinctive design, graphics, logo, symbols, words, or any combination thereof that exclusively identifies a firm and/or its goods or services.

4.2 Intellectual Property Laws

Intellectual property law is a law which protects the property under federal law. The owner has been granted certain exclusive right which includes copyright, patent, trademarks, license, and inventor a chance to control the use of innovative self creations. helpful and legal way of providing the It could be in the form of any intangible asset, idea or expression, data, formula, industrial design right, music, identification sign of software program.

The general laws in relation to Intellectual Property Enforcement in India are mainly the following:-

- The Code Of Civil Procedure
- The Indian Penal Code
- The Civil and Criminal Rules of Practice

The Intellectual Property Laws do provide for statutory enforcement mechanisms. The most important of the Indian Intellectual Property Laws are:-

- The Patents Act, 1970

- The Trade Marks Act, 1999
- The Copyright Act, 1957 &
- The Designs Act, 2001

The above legislations are supported by the relevant Rules there under and these rules are:-

- The Patents Rules, 1972 as amended by the Patents (Amendment) Act of 1999
- The Trade Rules, 2001
- The Copyright Rules, 1958 &
- The Designs Rules, 2000

The main post WTO Intellectual Property legislations are:

- The Geographical Indications Act, 1999
- The Semi Conductors Integrated Circuits Layout -Design Act, 2000

The Geographical Indications Rules provide the administrative mechanisms for registration and enforcement of Geographical Indications. The Semi Conductor Integrated Circuits Lavout Design Act is yet to have its rules to support the administrative mechanism there under. The Information Technology Act, 2000 also plays an important role in relation to areas of inter-phase between Information Technology and Intellectual Property Rights.

4.3 Intellectual Property Law Firms

There are many big and small intellectual property law firm worldwide, like in India, USA, UK, Chicago, Dubai, California, Boston etc, providing qualitative help to inventors and creators of products. These law firms are equipped with highly qualified professionals and provide legal help to their clients for valuation of intellectual property rights.

The World Intellectual Property Organization

The World Intellectual Property Organization (WIPO) is one of the specialized agencies of the United Nations (UN). The convention establishing the "World Intellectual Property Organization" was signed at Stockholm in 1967 and entered into force in 1970. Intellectual property shall include rights relating to:

- literary, artistic and scientific works,
- performances of performing artists, phonograms and broad casts,
- inventions in all fields of human endeavor,
- scientific discoveries,
- industrial designs,
- trademarks, service marks and commercial names and designations,
- protection against unfair competition, and
- all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.

4.5 Mission Mission of WIPO

The mission of WIPO is to promote through international cooperation in the creation, dissemination, use and protection of works of the human mind for the economic, cultural and social progress of all mankind. Its effect is to contribute to a balanc between the stimulation of creativity worldwide, by sufficien protecting the moral and material interests of creators on the one hand, and providing access to the socio-economic and cultur benefits of such creativity worldwide on the other.

WIPO's place on the international scene has greatly changed since its beginnings, when it was created to serve as the secretariat of treaties concluded between the states. Although WIPO has maintained this function (it currently administers 23 such treaties), together with the consequential one of promoting intergovernmental cooperation in the administration of intellectual property, its activities have not only expanded, bu also greatly diversified.

An outstanding example of the expansion of WIPO's earlier work is the growth of its registration activities that is to say, the increase in the use of international treaties that create the

facility of a single procedure to apply for patents and register trademarks and industrial designs, valid to all states party to those treaties.

4.6 Global Innovation Index (GII)

The Global Innovation Index (GII) was launched by INSEAD in 2007. It serves as recognition of the key role that innovation acknowledgement of the need for a broad horizontal vision of serves as a driver of economic growth and prosperity. It is also an innovation that is applicable to both developed and emerging economies, with the inclusion of indicators that go beyond the traditional measures of innovation (such as the level of research and development in a given country).

The GII is a valuable benchmarking tool to facilitate public-private dialogue, whereby policymakers, business leaders and other stakeholders can evaluate progress on a continual basis.

4.7 Advantages of GII

Advantages of GII are:

1. It determines the metrics and approaches for the capture of the richness of innovation in society.

2. It helps to make continual evaluation of innovative factor.

3. It provides a key tool and a rich database of detailed metrics for refining innovation policies.

4. The great emphasis is placed on measuring the climate and infrastructure for innovation and on assessing related outcomes.

5. With the end results, it forms several rankings,

6. It is more concerned with improving the journey' to better measuring and understanding innovation, and with identifying targeted policies, good practices, and other levers to foster innovation.

Thus, the expertise of the GII's Knowledge Partners and the prominent Advisory Board, the Gll model is continually updated to reflect the improved availability of statistics.

The top 10 countries in the GII 2012 edition are Switzerland, Singapore, Sweden, Finland, the UK, the Netherlands, Denmark Hong Kong (China), Ireland, and the United States of America (USA).

4.8 Electronic Copyright Management System (ECMS)

Electronic Copyright Management System (ECMS) is otherwise called Digital Rights Management (DRM). ECMS is a technology that creates certain conditions about how some digital products can be used and shared. It was set up as a system for the protection of digital works.

Mostly "secure transmission" of digital materials between sender and recipient over the network is done by means of encryption. The authorized recipient of the material can be required to make a payment to the owner before obtaining the key. Once the key is obtained, the recipient can decrypt the material and make use of it. ECMS cannot prevent the recipient from further circulating with the same decoding key (if the owner uses the same key for all encryption).

4.9Advantages of ECMS

The following are the advantages of ECMS:

1. A stronger degree of protection can be created with a centralized source of access to copyrighted material.
2. It can prevent from copying without the authorization.
3. It is a form of continual protection that protects works and manages rights at all times, no matter where the works are located or who has possession of them.
4. It attempts to promote authorized use of a copyright work, in part by precluding the possibility of copyright infringement
5. It comprises s a a num number of technological components, which can include encryption, a surveillance mechanism, databases of works, owners and users, license management functionality and Technological Protection Measures (TPMS).
6. It makes the protected content available to the authorized user and controlls any

further use of the content.

4.10 Indian Copy Rights Act on Soft Property Works

Technology had, in the past, given birth to new forms of creative expressions in the creative arts which were subsequently brought under the purview of copyright protection.

i. Trade - Related Aspects of Intellectual Property Rights (TRIPS) incorporated as a provision as, "computer programs, whether in source or object code, shall be protected as literary works under the Berne convention.

WEPD 188 - Protectia of

ii. Computer databases are covered by the definition of literary works in the Indian Act.

iii. Multimedia works, being a digital product and classified as computer programs, have a separate provisions for rights and ownership.

iv. Rights of digital reproduction covered in the cases of literary dramatic and musical works in the Indian Copyright Ac where the expression 'reproduction' includes "the storing of it in any medium by electronic means".

Copyright as provided by the Indian Copyright Act is valid only within the borders of the country. To secure protection to Indian works in foreign countries, India has become a member of the following international conventions on copyright and related rights:

- Berne Convention for the protection of literary and artistic works.
- Universal copyright convention.
- Convention for the protection of procedures of phonograms against unauthorized duplication of their programs.
- Multilateral convention for the avoidance of double taxation of copyright royalties.
- Trade related aspects of Intellectual Property Rights (TRIPS) Agreement,

4.11 Indian Patents Act on Soft Property Works

A patent is an IPR that is granted for an invention. Thus, it is the exclusive right of an

inventor to prevent others from making, using or distributing the patented invention without his permission. Again the specific procedure and requirements of granting a patent differ from country to country. But a patent is granted only when the invention is essentially novel, useful and non-obvious. The Patents Act, 1970 governs patents in India which are granted for a period of twenty years. In India, no patent ais offered to a computer program, mathematical algorithm. Only copyright protection exists for a protection is computer program.

UNIT -III

EVIIDENCE ASPECTS

5.1 Computer crime

'Computer crime refers to any crime that involves computer and a network".

Crimes based on electronic offences are bound to increase.

Cyber crimes are categorized in two ways

1. The Computer as a Target:-using a computer to attack other computers.

   E.g. Hacking, Virus/Worm attacks, DOS attack etc.

2. The computer as a weapon:-using a computer to commit real world crimes.

5.2 Criminal activities

Technological advancements have created new possibilities for criminal activities. Some of the criminal activities are:

d. E-mail related crimes

1. Email spoofing

Email spoofing refers to email that appears to have been originated from one source but actually sent from another source.

2. Email Spamming

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3. Sending malicious codes through email

Viruses, trojans etc are sent through emails as an attachment or through the link of a website.

4. Email bombing

E-mail “bombing” is a respeatedly sent an identical email message to a particular address in an irritating manner.

5. Sending threatening emails

6. Defamatory emails

7. Email frauds

5.3 Factors influencing computer crimes

The following factors could induce computer crimes:

1. The expansion of worldwide access to the Internet.
2. Very limited knowledge of the computer network infrastructure.
3. Inherent weakness of cyberspace infrastructure and communication protocols.
4. Outdated laws and statutory limitations.
5. Absence of comprehensive law.
6. No law enforcement for the new technological challenge.
7. No Harmonization for international standards of computer usage and conduct.
8. Lack of adequate training diminishes the investigative capacity of police agencies.
9. No proper reporting mechanism to government agencies
10. Detecting the computer crime is very challenging to organizations and investigators.
11. In the private sector, there is very little interest in reporting of any system related intrusions. This is a result of the fear of marketplace forces that would expose management's weaknesses to the shareholder community and competitors.

5.4 Strategy for prevention of computer crimes

The following are the strategies that can be applied to prevent computer crimes

1.Cyber security

Cyber security is one of the mechanism through which cyber crimes can be prevented. It involves protection of sensitive personal and business information through prevention, detection and response to different online attacks.

2.Privacy policy

While designing the website, some may incorporate the privacy policy statement and in other cases they might not have incorporated the same. So, it is essential for the user to look over the site's privacy policy statement before submitting the personal information such as name, e mail address, telephone number, online payment details.

3.Encryption

Personal information can be encrypted while submitting through online to protect attackers from hijacking the information. Probably in majority of the websites, Secure Socket Layer (SSL) is adopted to encrypt information. So it is advisable to utilize such websites which "garbles" the data to make it unintelligible to anyone who tries to hack into the computer system.

4.Updating of software

Updating the existing software or installing new software cam prevent attackers from being able to take advantage.

5. Usage of good passwords

Password can be created in such a way that no stranger could guess the password. Apart from that, utmost care must be taken to see that one should not give the option to the computer remember the password on its own.

6. Disable remote connectivity

Some Personal Digital Assistant and phones are equipped with wireless technologies, such as Bluetooth, Wi-Fi which can be used to connect other devices or computers. Disabling these features when they are not in use will protect the user's devices from attacks.

7.Turning on spam blocker

The user can apply a spam blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails

8. Adoption of anti-virus software

Having adequate anti-virus software for the computer, such as McAfee, Norton Anti-Virus, Stopzilla or other similar programs and updating the anti-virus software once in a week. will help to prevent from any trojan, spyware, viruses and other problems.

9. Firewall Protection

With the use of computer's firewall protection feature (digitally created barrier), the user can prevent the hackers from getting into the computer system.

10. Usage of secured website

Online shopping done on a secured website, like those with a URL (Uniform Resource Locator) that starts with "https" and/or have VeriSign seal will protect the personal information and ensures privacy. If it is not found anywhere in the site, submitting the credit card information and other personal information to a site will be risky.

11. Cautious in sweepstakes

Cyber criminals are using common scams such as foreign lotteries, phony sweepstakes and other similar methods to get the personal information and money. So the users should not get attracted by these offers.

5.5 The Indian Evidence Act

The advent of information technology has brought into existence a new kind of document called the electronic record. This document can preserve in same quality and stay for a long period of time through encryption processes reducing the chance of tampering of evidence. This document can be in various forms like a simple e-mail or short message or multimedia message or other electronic forms.

The Indian Evidence Act, originally passed by the British Parliament in 1872, contains a set of rules and allied issues governing admissibility of evidence in the Indian courts of law.

5.6 Evidence aspects as part of the law of procedures

The Indian Evidence Act, 1872 and Information Technology Act, 2000 grants legal recognition to electronic records.

According to section 2(t) of the Information Technology Act, 2000 "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. The Act recognizes electronic record in a wide sense thereby including electronic data in any form such as videos or voice messages.

- The information technology has made it easy te communicate and transmit data in various forms from a simple personal computer or from a mobile phone or from other kinds of devices.

- The Information Technology Amendment Act, 2008 has recognized various forms of communication devices and defines a "communication device" under section 2 (ha) of the Act "communication device" to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

- The Indian Information Technology Act 2000 lays down a blanket permission for records not to be denied legal effect if they are in electronic form as long as they are accessible for future reference.

5.7 Applicability of the law of evidence on electronic records

The Indian Evidence Act under Section 3, Section 65A and Section 65B which is admissible for electronic records.

- Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records. According to section 3 of the Act,

'Evidence' means and includes-

(1) All statements which the court permits or requires to be made before it by witness, in relation to matters of fast under inquiry; such statement is called oral evidence,

(2) All documents including electronic records produced for the inspection of the Court;

such documents are called documentary evidence.

From the aforesaid provisions it becomes amply clear that the law, as it prevails today, takes care of information stored on magnetic or electronic device and treats it as documentary evidence within the meaning of section 3 of the Indian Evidence Act.

- Further, in section 4, the Information Technology Act 2000 provides:

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) made available in an electronic form, and

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

- 65A. Special provisions as to evidence relating to electronic record:

The contents of electronic records may be proved in accordance with the provisions of section 65B.

- 65B. Admissibility of electronic records:

-any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document.

- Conditions for admissibility

- the computer output containing the information was produced by the computer during the period over which the computer was **used regularly** to store or process information for the purposes of any activities regularly carried on over that pe riod by the person having lawful control over the use of the com puter;

- during the said period, information of the kind contained in the electronic record or of the kind from which the informatice so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

- throughout the material part of the said period, the com puter was operating properly or, if not; then in respect of any period in which is propelering properly or was out of operation during that part of the period, was not such as to affed the electronic record or the accuracy of its contents;

- the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

5.9 The Indian Penal Code, 1860

Indian Penal Code (IPC) is the main criminal code of India. It was drafted in 1860 and came into operation in India on the 1st of January, 1862. It is a comprehensive code, intended to cover all substantive aspects of criminal law and deals specifically with offences, stating what matters will afford an excuse or a defence to a charge or an offence. It has since been amended several times and is now supplemented by other criminal provisions. Now, even cyber crimes can be punished under the code.

5.10 Amendments to the Indian Penal Code

1. After section 29, the following section shall be insertet namely:- "29 A. Electronic record. The words "electronic reconte shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames translates that document", the words "such public servant, changes with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in Court of Justice", the words "produce a document or an electronis record in a court of Justice" shall be substituted.

4. In section 173. for the words "to produce a document ins Court of Justice" the words "to produce a document of electronic record in Court of Justice" shall be substituted.

5. In section 175. for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in book or record, or makes any

document containing a fals statement", the words "makes any false entry in any book or record or electronic record or makes any document or electronic recording containing a false statement shall be substituted.

7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In section 463, for the words "Whoever makes any false documents or part of a document with intent to cause damage or tinjury", the words "Whoever makes any false documents or false electronic record or party of a document or electronic record, with intent to cause damage or injury" shall be substituted.

9. In section 464,- (a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the documents or the nature of the alteration", the following shall be substituted, namely:-

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority or a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; (or)

Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made. executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; (or)

Who dishonestly or fraudulently causes any person, sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such or that by reason of deception practised upon him, he does not person by reason of unsoundness of

mind or intoxication cannot know the contents of the document or electronic record or the nature of the alteration".

10. In section 466,-

(a) for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted.

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forge" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 471, for the word "document" whenever it occurs, the words "document or electronic record" shall be substituted

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words " if the document is one of the description mentioned in section 466 of this Code" the following shall be substitute, namely

“Wheever has in his possession any document or electronic mont knowing the same to be forged and intending that the same shil fraudulently or dishonestly be used as a genuine, shall, The document or electronic record is one of the description mentioned in secttion 406 of this Code."

16. in section 476, for the words "any document", the words "my document or electronic record" shall be substituted.

17. In section 477a, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic mand, paper, writing" shall be substituted.

Snapshot of Important Cyber law Provisions in India

Offence	**Section under IT Act**
Tampering with Computer source documents	Sec.65

Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

Computer Related Crimes Covered under Indian Penal Code and Special Laws

Offence	Section
Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec 463 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 463 IPC
Web-Jacking	Sec 383 IPC
E-Mail Abuse	Sec 500 IPC
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

Source: http://www.cyberlawclinic.org/cyberlaw.htm

INDIAN EVIDENCE ACT, 1872

1. Introduction

The Indian Evidence Act, 1872 lays down the rules of evidence which govern the admissibility, relevance, and proof of facts in Indian courts. It ensures that judicial decisions are based on reliable and legally acceptable evidence.

Enacted: 1872

Enforced: 1st September 1872

Applies to: Whole of India

Objective: To consolidate and define the law of evidence

2. Meaning of Evidence (Section 3)

Evidence includes

Oral Evidence – Statements made by witnesses before the court.

Documentary Evidence – Documents produced for inspection by the court.

3. Facts (Section 3)

Fact: Anything capable of being perceived by senses.

Relevant Fact: A fact connected with the fact in issue.

Facts in Issue: Facts that determine the outcome of a case.

4. Structure of the Act

The Act contains 167 Sections divided into 3 Parts:

PART I – RELEVANCY OF FACTS (Sections 1–55)

Important Concepts:

Relevant Facts (Sections 5–55)

Evidence must relate to facts in issue or relevant facts

Types of Relevant Facts:

Facts forming part of same transaction (Res Gestae) – Sec 6

Admissions – Sec 17

Confessions – Sec 24–30

Statements by persons who cannot be called as witnesses – Sec 32 (Dying Declaration)

Opinions of experts – Sec 45

Character Evidence – Sec 52–55

PART II – PROOF (Sections 56–100)

A. Oral Evidence (Sections 59–60)

Must be direct evidence

Hearsay evidence is generally not admissible

B. Documentary Evidence (Sections 61–90A)

Primary Evidence – Original document

Secondary Evidence – Copies, certified copies

C. Burden of Proof (Sections 101–114A)

Burden lies on the person who asserts a fact

Presumption of facts – Sec 114

Estoppel – Sec 115

PART III – PRODUCTION & EFFECT OF EVIDENCE (Sections 101–167)

Important Topics:

Witnesses – Sec 118

Competency of witnesses

Examination of witnesses

Examination-in-chief

Cross-examination

Re-examination

Hostile Witness

Privileges of witnesses

5. Confession

A confession is an admission of guilt.

Confession made under threat, inducement, or promise is inadmissible.

Police confession is generally not admissible.

6. Dying Declaration (Section 32)

Statement made by a person about the cause of their death.

Admissible even if the person is dead.

No oath required**.**

7. Admissions (Section 17)

A statement suggesting an inference as to a fact in issue.

Admissions are relevant but not conclusive proof.

8. Witnesses

Any person capable of understanding questions can be a witness.

Includes child witnesses, expert witnesses, and hostile witnesses.

9. Presumption

Presumption of fact

Presumption of law

Conclusive proof

10. Importance of the Indian Evidence Act

Ensures fair trial

Prevents arbitrary decisions

Brings uniformity in judicial proceedings

Protects rights of parties

11. Conclusion

The Indian Evidence Act, 1872 is the backbone of the Indian judicial system, ensuring that justice is delivered based on credible, relevant, and legally

COMPUTER CRIME (CYBER CRIME)

1. Meaning

Computer crime refers to illegal activities in which a computer, computer system, or computer network is used as a tool, target, or place of crime.

2. Definition

Cyber Crime is any unlawful act committed using computers, digital devices, or the internet, where data or systems are attacked, misused, or manipulated**.**

3. Characteristics of Computer Crime

Technology-driven

Borderless in nature

Anonymous offenders

High speed and automation

Difficult to detect and prove

4. Types of Computer Crime

A. Crimes Against Individuals

Cyber stalking

Online harassment

Identity theft

Email spoofing

Cyber defamation

B. Crimes Against Property

Hacking

Data theft

Malware attacks

Ransomware

Intellectual property theft

Software piracy

C. Crimes Against Organizations

Denial of Service (DoS) attacks

Website defacement

Corporate espionage

Insider attacks

D. Crimes Against Government

Cyber terrorism

Hacking government websites

Espionage

Attacks on critical infrastructure

5. Common Forms of Computer Crime

Hacking – Unauthorized access to systems

Phishing – Fraudulent emails to steal data

Malware – Viruses, worms, trojans

Ransomware – Data encrypted for ransom

Spamming

Online fraud

Data diddling

Salami attacks

6. Computer Crime under Indian Law

Information Technology Act, 2000 (Amended 2008)

Section	Offence
Sec 43	Unauthorized access, data damage
Sec 65	Tampering with computer source code
Sec 66	Computer-related offences
Sec 66C	Identity theft
Sec 66D	Cheating by personation
Sec 66E	Violation of privacy
Sec 66F	Cyber terrorism
Sec 67	Publishing obscene content

7. Punishments

Imprisonment

Fine

Compensation to victims

Both imprisonment and fine

8. Challenges in Controlling Computer Crime

Lack of technical expertise

Jurisdiction issues

Rapid technological changes

Inadequate cyber awareness

Evidence preservation difficulties

9. Prevention of Computer Crime

Strong passwords and authentication

Regular software updates

Firewalls and antivirus

Cyber awareness training

Data encryption

Legal compliance

10. Role of Cyber Forensics

Collection of digital evidence

Analysis of logs and metadata

Tracking cyber criminals

Supporting legal proceedings

11. Conclusion

Computer crime poses a serious threat to individuals, organizations, and national security. Effective laws, advanced technology, and public awareness are essential to combat cyber crime.

FACTORS INFLUENCING COMPUTER CRIMES

1. Rapid Growth of Technology

Fast expansion of computers, smartphones, and the internet

New technologies create new vulnerabilities

Security measures often lag behind innovation

2. Easy Access to Computers and Internet

Widespread availability of devices

Public Wi-Fi and unsecured networks

Affordable internet increases exposure to cyber threats

3. Lack of Cyber Awareness

Users unaware of cyber risks

Poor password practices

Falling victim to phishing and fraud

4. Weak Security Systems

Outdated software

Lack of firewalls and antivirus protection

Poor system configuration

5. Anonymity on the Internet

Offenders can hide identity

Use of fake profiles, VPNs, and dark web

Difficult to trace criminals

6. Financial Gain

Online fraud and scams for money

Ransomware attacks

Theft of banking and credit card data

7. Insider Threats

Employees misuse access privileges

Disgruntled or careless insiders

Lack of monitoring and controls

8. Inadequate Cyber Laws and Enforcement

Weak implementation of laws

Low conviction rates

Jurisdictional issues across countries

9. Global Nature of Cyber Space

Crimes cross national borders

Different legal systems

Difficulty in international cooperation

10. Curiosity and Thrill-Seeking Behavior

Hackers seeking challenge or recognition

Young offenders experimenting with technology

11. Poor Digital Ethics

Lack of moral responsibility

Software piracy culture

Unauthorized data access seen as harmless

12. Lack of Cyber Policing and Expertise

Shortage of trained cyber crime professionals

Limited forensic infrastructure

13. Social Engineering Tactics

Manipulation of human psychology

Trust exploitation rather than technical hacking

14. Increase in Online Transactions

Growth of e-commerce and digital banking

More sensitive data stored online

Conclusion

Computer crimes are influenced by technological, social, economic, and legal factors. Combating them requires strong laws, robust security, skilled professionals, and cyber awareness among users.

STRATEGIES FOR PREVENTION OF COMPUTER CRIME

1. Technical Strategies

Use strong passwords and multi-factor authentication

Install and regularly update antivirus and anti-malware

Use firewalls and intrusion detection systems

Encrypt sensitive data

Regular system updates and patch management

Secure Wi-Fi networks

2. Administrative and Organizational Strategies

Establish clear IT security policies

Define access control and user privileges

Conduct regular security audits

Maintain logs and monitoring systems

Implement data backup and recovery plans

3. Legal and Regulatory Strategies

Strict enforcement of the Information Technology Act, 2000

Strong cyber laws with deterrent punishments

International cooperation for cross-border crimes

Mandatory compliance standards (ISO, CERT-In guidelines)

4. Awareness and Training

Cyber awareness programs for users

Training employees on phishing and social engineering

Promote ethical use of technology

Inclusion of cyber security education in curriculum

5. Cyber Policing and Investigation

Strengthening cyber crime cells

Training law enforcement officers

Use of cyber forensics tools

Quick response mechanisms

6. Preventive Strategies for Individuals

Avoid sharing personal information online

Verify emails and links before clicking

Use secure payment gateways

Regularly check bank statements and accounts

7. Preventive Strategies for Organizations

Regular vulnerability assessments

Role-based access control

Insider threat management

Incident response teams

8. Role of Government

National cyber security policy

CERT-In coordination

Public awareness campaigns

Collaboration with private sector

9. International Cooperation

Treaties and information sharing

Joint cyber crime investigations

Global cyber security standards

INDIAN EVIDENCE ACT, 1872

1. Introduction

The Indian Evidence Act, 1872 lays down the rules of evidence which govern the admissibility, relevance, and proof of facts in Indian courts. It ensures that judicial decisions are based on reliable and legally acceptable evidence.

Enacted: 1872

Enforced: 1st September 1872

Applies to: Whole of India

Objective: To consolidate and define the law of evidence

2. Meaning of Evidence (Section 3)

Evidence includes:

Oral Evidence – Statements made by witnesses before the court.

Documentary Evidence – Documents produced for inspection by the court.

3. Facts (Section 3)

Fact: Anything capable of being perceived by senses.

Relevant Fact: A fact connected with the fact in issue.

Facts in Issue: Facts that determine the outcome of a case**.**

4. Structure of the Act

The Act contains 167 Sections divided into 3 Parts:

PART I – RELEVANCY OF FACTS (Sections 1–55)

Important Concepts:

Relevant Facts (Sections 5–55)

Evidence must relate to facts in issue or relevant facts

Types of Relevant Facts:

Facts forming part of same transaction (Res Gestae) – Sec 6

Admissions – Sec 17

Confessions – Sec 24–30

Statements by persons who cannot be called as witnesses – Sec 32 (Dying Declaration)

Opinions of experts – Sec 45

Character Evidence – Sec 52–55

PART II – PROOF (Sections 56–100)

A. Oral Evidence (Sections 59–60)

Must be direct evidence

Hearsay evidence is generally not admissible

B. Documentary Evidence (Sections 61–90A)

Primary Evidence – Original document

Secondary Evidence – Copies, certified copies

C. Burden of Proof (Sections 101–114A)

Burden lies on the person who asserts a fact

Presumption of facts – Sec 114

Estoppel – Sec 115

PART III – PRODUCTION & EFFECT OF EVIDENCE (Sections 101–167)

Important Topics:

Witnesses – Sec 118

Competency of witnesses

Examination of witnesses

Examination-in-chief

Cross-examination

Re-examination

Hostile Witness

Privileges of witnesses

5. Confession

A confession is an admission of guilt.

Confession made under threat, inducement, or promise is inadmissible.

Police confession is generally not admissible.

6. Dying Declaration (Section 32)

Statement made by a person about the cause of their death.

Admissible even if the person is dead.

No oath required.

7. Admissions (Section 17)

A statement suggesting an inference as to a fact in issue.

Admissions are relevant but not conclusive proof.

8. Witnesses

Any person capable of understanding questions can be a witness.

Includes child witnesses, expert witnesses, and hostile witnesses.

9. Presumptions

Presumption of fact

Presumption of law

Conclusive proof

10. Importance of the Indian Evidence Act

Ensures fair trial

Prevents arbitrary decisions

Brings uniformity in judicial proceedings

Protects rights of parties

COMPUTER CRIME (CYBER CRIME)

1. Meaning

Computer crime refers to illegal activities in which a computer, computer system, or computer network is used as a tool, target, or place of crime.

2. Definition

Cyber Crime is any unlawful act committed using computers, digital devices, or the internet, where data or systems are attacked, misused, or manipulated.

3. Characteristics of Computer Crime

Technology-driven

Borderless in nature

Anonymous offenders

High speed and automation

Difficult to detect and prove

4. Types of Computer Crime

A. Crimes Against Individuals

Cyber stalking

Online harassment

Identity theft

Email spoofing

Cyber defamation

B. Crimes Against Property

Hacking

Data theft

Malware attacks

Ransomware

Intellectual property theft

Software piracy

C. Crimes Against Organizations

Denial of Service (DoS) attacks

Website defacement

Corporate espionage

Insider attacks

D. Crimes Against Government

Cyber terrorism

Hacking government websites

Espionage

Attacks on critical infrastructure

5. Common Forms of Computer Crime

Hacking – Unauthorized access to systems

Phishing – Fraudulent emails to steal data

Malware – Viruses, worms, trojans

Ransomware – Data encrypted for ransom

Spamming

Online fraud

Data diddling

Salami attacks

6. Computer Crime under Indian Law

Information Technology Act, 2000 (Amended 2008)

Section	Offence
Sec 43	Unauthorized access, data damage
Sec 65	Tampering with computer source code
Sec 66	Computer-related offences
Sec 66C	Identity theft
Sec 66D	Cheating by personation
Sec 66E	Violation of privacy
Sec 66F	Cyber terrorism

Sec 67 Publishing obscene content

7. Punishments

Imprisonment

Fine

Compensation to victims

Both imprisonment and fine

8. Challenges in Controlling Computer Crime

Lack of technical expertise

Jurisdiction issues

Rapid technological changes

Inadequate cyber awareness

Evidence preservation difficulties

9. Prevention of Computer Crime

Strong passwords and authentication

Regular software updates

Firewalls and antivirus

Cyber awareness training

Data encryption

Legal compliance

10. Role of Cyber Forensics

Collection of digital evidence

Analysis of logs and metadata

Tracking cyber criminals

Supporting legal proceedings

FACTORS INFLUENCING COMPUTER CRIMES

1. Rapid Growth of Technology

Fast expansion of computers, smartphones, and the internet

New technologies create new vulnerabilities

Security measures often lag behind innovation

2. Easy Access to Computers and Internet

Widespread availability of devices

Public Wi-Fi and unsecured networks

Affordable internet increases exposure to cyber threats

3. Lack of Cyber Awareness

Users unaware of cyber risks

Poor password practices

Falling victim to phishing and fraud

4. Weak Security Systems

Outdated software

Lack of firewalls and antivirus protection

Poor system configuration

5. Anonymity on the Internet

Offenders can hide identity

Use of fake profiles, VPNs, and dark web

Difficult to trace criminals

6. Financial Gain

Online fraud and scams for money

Ransomware attacks

Theft of banking and credit card data

7. Insider Threats

Employees misuse access privileges

Disgruntled or careless insiders

Lack of monitoring and controls

8. Inadequate Cyber Laws and Enforcement

Weak implementation of laws

Low conviction rates

Jurisdictional issues across countries

9. Global Nature of Cyber Space

Crimes cross national borders

Different legal systems

Difficulty in international cooperation

10. Curiosity and Thrill-Seeking Behavior

Hackers seeking challenge or recognition

Young offenders experimenting with technology

11. Poor Digital Ethics

Lack of moral responsibility

Software piracy culture

Unauthorized data access seen as harmless

12. Lack of Cyber Policing and Expertise

Shortage of trained cyber crime professionals

Limited forensic infrastructure

13. Social Engineering Tactics

Manipulation of human psychology

Trust exploitation rather than technical hacking

14. Increase in Online Transactions

Growth of e-commerce and digital banking

More sensitive data stored online

STRATEGIES FOR PREVENTION OF COMPUTER CRIME

1. Technical Strategies

Use strong passwords and multi-factor authentication

Install and regularly update antivirus and anti-malware

Use firewalls and intrusion detection systems

Encrypt sensitive data

Regular system updates and patch management

Secure Wi-Fi networks

2. Administrative and Organizational Strategies

Establish clear IT security policies

Define access control and user privileges

Conduct regular security audits

Maintain logs and monitoring systems

Implement data backup and recovery plans

3. Legal and Regulatory Strategies

Strict enforcement of the Information Technology Act, 2000

Strong cyber laws with deterrent punishments

International cooperation for cross-border crimes

Mandatory compliance standards (ISO, CERT-In guidelines)

4. Awareness and Training

Cyber awareness programs for users

Training employees on phishing and social engineering

Promote ethical use of technology

Inclusion of cyber security education in curriculum

5. Cyber Policing and Investigation

Strengthening cyber crime cells

Training law enforcement officers

Use of cyber forensics tools

Quick response mechanisms

6. Preventive Strategies for Individuals

Avoid sharing personal information online

Verify emails and links before clicking

Use secure payment gateways

Regularly check bank statements and accounts

7. Preventive Strategies for Organizations

Regular vulnerability assessments

Role-based access control

Insider threat management

Incident response teams

8. Role of Government

National cyber security policy

CERT-In coordination

Public awareness campaigns

Collaboration with private sector

9. International Cooperation

Treaties and information sharing

Joint cyber crime investigations

Global cyber security standards

Prevention of computer crime requires a multi-layered strategy involving technology, law, education, and international cooperation. Proactive prevention is more effective than reactive punishment.

Amendments to Indian Penal Code 1820

1. Historical Amendments to IPC (Before Replacement)

The IPC, since enactment in 1860, was amended repeatedly by Parliament over many years. Important legislative changes included:

◆ Pre-Independence Amendments

Various amendment acts between 1870 to 1943 modifying specific sections and updating penal provisions (e.g., Sedition Section 124A introduced in 1870s)

◆ Post-Independence Amendments

Some major acts that changed IPC provisions after 1947

Criminal Law (Amendment) Act, 1952 – modifications to criminal law provisions.

Indian Penal Code (Amendment) Acts (1959, 1961, 1969) – amendments to various IPC sections.

Criminal Law (Amendment) Act, 1972 – changes to offences and punishments.

Criminal Law (Amendment) Acts, 1983 – included dowry weapon provisions and victim protections.

The Dowry Prohibition (Amendment) Act, 1986 – impacted IPC sections relating to dowry death and cruelty.

Criminal Law (Amendment) Act, 1993 – further updates to IPC offences.

2. Major Recent Amendments (21st Century)

◆ Information Technology Act, 2000

Although not strictly an "IPC amendment act," this law amended certain IPC provisions to address cyber issues and extended definitions where computer crimes could fall under IPC categories.

Wikipedia

3. Criminal Law (Amendment) Act, 2013

Often called the Nirbhaya Amendment, this was one of the most significant modern amendments to the IPC (and CrPC, Evidence Act):

Introduced new offences related to gender-based crimes including:

• Acid attack (Sections 326A & 326B)

• Sexual harassment (Section 354A)

• Voyeurism (Section 354C)

• Stalking (Section 354D)

• Attempt to disrobe (Section 354B)

• Sexual assault causing death or vegetative state (Section 376A)

Strengthened punishment for rape and related crimes.

This Act was passed in 2013 after the Nirbhaya gang-rape case to make laws on sexual violence more stringent.

4. Criminal Law (Amendment) Act, 2018

This amendment targeted rape laws, including:

PRS Legislative Research

Increased minimum punishment for rape of women.

Introduced harsher penalties for rape of girls under 12 and 16 years (with 20 years to life or death penalty for very young victims).

PRS Legislative Research

It also added new IPC sections and modified existing ones (e.g., Sections 376AB, 376DA, 376DB — addressing gang rape and child rape specifics) and amended protective sections like 228A (identity of victims) and 166A (public servants disobeying law).

iPleaders

5. Replacement by Bharatiya Nyaya Sanhita, 2023

The Indian Penal Code ceased to apply from 1 July 2024, being replaced by the Bharatiya Nyaya Sanhita (BNS), 2023 as the new criminal code of India.

BNS repealed the IPC and introduced a new structure.

It adds, modifies, or removes many offences and punishments.

Many IPC sections have been replaced, renumbered, or re-conceptualized within BNS.

Criminal Law (Amendment), 2018

Harsher rape punishments and age-specific rape provisions

PRS Legislative Research

Information Technology Act, 2000	Extended cyber definitions impacting IPC enforcement
Numerous historical amendments	Updated penal provisions over decades
Replacement by BNS, 2023	New criminal code replacing IPC 1860

UNIT -IV

Legal Framework for EDI (Electronic Data Interchange)

Electronic Data Interchange (EDI) refers to the electronic exchange of business documents (such as invoices, purchase orders, shipping notices) between organizations in a standardized digital format. To ensure security, authenticity, and legal validity, EDI operates within a well-defined legal framework.

1. Information Technology Act, 2000 (India)

The IT Act is the backbone of EDI's legal recognition in India.

Gives legal validity to electronic records and electronic contracts

Recognizes digital signatures as valid authentication

Section 4: Legal recognition of electronic records

Section 5: Legal recognition of digital signatures

Section 10-A: Validity of contracts formed through electronic means

Ensures that EDI documents are treated at par with paper documents.

2. Indian Evidence Act, 1872 (Amended)

Electronic records are recognized as admissible evidence

Section 65-B: Conditions for admissibility of electronic records

EDI messages can be produced as evidence in courts

3. Indian Contract Act, 1872

Contracts formed via EDI are valid if essentials of a valid contract are met:

Offer and acceptance

Free consent

Lawful consideration

Lawful object

Supports electronic contracts (e-contracts)

4. Digital Signature & Authentication Laws

Use of Digital Signature Certificates (DSC) issued by licensed Certifying Authorities

Ensures:

Authenticity of sender

Integrity of data

Non-repudiation

5. UNCITRAL Model Laws

India follows international standards laid down by:

UNCITRAL Model Law on Electronic Commerce (1996)

UNCITRAL Model Law on Electronic Signatures (2001)

These promote:

6.**Uniformity in international EDI transactions**

Legal acceptance of electronic documents across borders

Cyber Laws and Data Protection

Protection against unauthorized access, data tampering, and cyber fraud

Sections 43 & 66 of IT Act deal with cyber offenses

Emphasizes confidentiality and security of EDI transactions

7. Banking and Commercial Regulations

RBI guidelines for electronic payments and digital transactions

EDI used in:

Customs clearance

Banking transactions

Supply chain and logistics

8. EDI Trading Partner Agreements

Organizations entering EDI arrangements define:

Legal responsibilities of parties

Data security standards

Dispute resolution mechanism

Liabilities and limitations

EDI Mechanism (Electronic Data Interchange Mechanism)

The EDI mechanism explains the step-by-step process through which business documents are exchanged electronically between organizations in a standardized, secure, and automated manner.

1. Preparation of Business Document

Business transaction is initiated (e.g., purchase order, invoice)

Data is entered into the sender's internal system (ERP / accounting software)

Example: Buyer creates a Purchase Order (PO)

2. Translation into EDI Standard Format

Internal data is converted into a standard EDI format

Common standards:

ANSI X12

EDIFACT

XML / EDI-XML

Done using EDI translation software

- Ensures compatibility between different computer systems

3. Communication / Transmission

Translated EDI message is transmitted to the receiver through:

Value Added Network (VAN)

Internet (AS2, FTP, SFTP)

Security features:

Encryption

Authentication

Digital signatures

4. Reception of EDI Document

Receiver's EDI system receives the message

Acknowledgement (Functional Acknowledgement – 997 / CONTRL) is sent back to confirm receipt

5. Translation into Receiver's Internal Format

EDI message is translated from standard format into:

Receiver's internal application format

Automatically integrated into ERP / business system

6. Processing of Transaction

Business action takes place:

Order processing

Inventory update

Shipment initiation

Payment processing

7. Storage and Audit Trail

EDI records are stored electronically

Maintains:

Legal evidence

Audit trail

Compliance with IT Act & Evidence Act

Flow of EDI Mechanism (Simple Diagram Explanation)

Sender System → EDI Translator → Secure Network → EDI Translator → Receiver System

Key Components of EDI Mechanism

Sender & Receiver systems

EDI translation software

Communication network

Security controls

Standard formats

Advantages of EDI Mechanism

Faster transactions

Reduced paperwork

Lower errors

Cost efficiency

Improved business relationships

EDI Scenario in India

Electronic Data Interchange (EDI) in India has evolved as a critical component of e-governance, trade facilitation, customs automation, banking, and supply-chain management. The Government

of India has actively promoted EDI to improve transparency, efficiency, and speed in commercial and regulatory transactions.

1. Introduction of EDI in India

EDI was introduced in India in the 1990s

Initially implemented in customs and foreign trade

Objective:

Reduce paperwork

Speed up clearance procedures

Improve accuracy and transparency

2. EDI in Customs (ICEGATE System)

Indian Customs EDI System (ICES) is the largest EDI implementation in India

Operated through ICEGATE (Indian Customs Electronic Gateway)

Functions:

Filing of Bills of Entry and Shipping Bills

Electronic payment of customs duty

Electronic clearance of import/export documents

Covers:

Major ports

Airports

Inland Container Depots (ICDs)

3. EDI in Foreign Trade

Used by:

Exporters

Importers

Customs House Agents (CHAs)

Linked with:

Directorate General of Foreign Trade (DGFT)

Banks

Shipping lines

Enables paperless trade transactions

4. EDI in Banking and Finance

Adopted by:

Commercial banks

RBI-regulated institutions

Applications:

Electronic fund transfers

Trade finance documents

Cheque truncation system (CTS)

NEFT / RTGS / ECS

Ensures faster and secure financial transactions

5. EDI in Taxation Systems

Income Tax Department:

E-filing of returns

Online tax payments

GST Network (GSTN):

Electronic filing of GST returns

E-invoicing and e-way bills

Reduces tax evasion and increases compliance

6. EDI in Railways and Transport

Indian Railways:

Freight operations

Online reservations

Transport sector:

Electronic permits

Logistics documentation

Improves coordination and tracking

7. EDI in Manufacturing and Supply Chain

Used by large enterprises and MNC

Integration with ERP systems (SAP, Oracle)

Applications:

Purchase orders

Invoices

Inventory management

Vendor-managed inventory (VMI)

8. Government Support and Legal Framework

Backed by:

Information Technology Act, 2000

Amendments to Evidence Act and IPC

Promoted under:

Digital India Initiative

Ease of Doing Business reforms

Adoption of international standards like EDIFACT

9. Challenges of EDI in India

High initial cost for SMEs

Lack of technical expertise

Infrastructure limitations in rural areas

Interoperability issues

10. Future Prospects of EDI in India

Integration with

Blockchain

AI-driven trade systems

Expansion in MSME sector

Full paperless trade environment

Cross-border EDI interoperability

The EDI scenario in India reflects a strong shift towards digital governance and automated trade processes. With robust government backing, legal recognition, and expanding infrastructure, EDI has become an essential tool for improving efficiency, transparency, and global competitiveness

UNIT-V

THE INFORMATION TECHNOLOGY ACT

Information Technology Act, 2000

The Information Technology Bill was passed in May 2000, in the houses of the Indian Parliament. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber law provisions are contained in the IT Act, 2000. Information Technology Act provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication.

7.5 Authentication of Electronic Records

The Information Technology Act, 2000 under Section 3 specifies that

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

(2) The authentication of the electronic record shall be effected by the use of asymmetric cryptosysltem and hash function which envelop and transform the initial electronic record into another electronic record] Explanation.- For the purposes of this sub-section," hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as" hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

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

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

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

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

7.6 Electronic Governance

The Information Technology Act, 2000 was enacted to "... provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bunkers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto

Thus, the focus of this Act is on electronic commerce and electronic records. The Act contains provisions on digital signatures and authentication of electronic records, legal recognition of digital signatures and electronic records, retention of electronic records, attribution, acknowledgement and dispatch of electronic records, security of electronic records, regulation of Certifying Authorities, Cyber Regulation Appellate Tribunal etc To facilitate the implementation of e-Governance projects at various levels across the country, a more holistic legal framework is required.

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-

- rendered or made available in an electronic form, and
- 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 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.

Explanation.-For the purposes of this section, "signed", with its grammatical variations and

cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Use of electronic records and digital signatures in Government and its Agencies

(1) 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 in a particular manner.
- the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner.
- the receipt or payment of money in a particular manner.

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, 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.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-

- the manner and format in which such electronic records shall be filed, created or issued.
- the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a)

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, if-93

- the information contained therein remains accessible so to be usable for a subsequent reference.
- the electronic record is retained in the format in which i was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received.

o 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:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

o Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Publication of rule, regulation, etc., in Electronic Gazette

Where any law provides that any rule, regulation, order, by-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, by-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, by-law, 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.

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-

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

Materials prepared by

Dr.B.Divya Keerthika & D.Amirthini

Assistant Professor
Department of Commerce with Professional Accounting and Department of Commerce
Vidyasagar College of Arts and Science
Udumalpet

Reference Books

- Cyber Law- Dr.B.Kirubashini – P. Kavitha
- Net Sources