

The Concept of Cyberspace

E-Commerce

- E-Commerce or Electronic Commerce means buying and selling of goods, products, or services over the internet.
- E-commerce is also known as electronic commerce or internet commerce.
- These services provided online over the internet network.
- *Transaction of money, funds, and data are also considered as E-commerce.*

★Key Characteristics of E-commerce:

- **Global Reach:** E-commerce transcends geographical boundaries, enabling businesses to reach customers worldwide without the constraints of physical location.
- **24/7 Availability:** E-commerce platforms are accessible 24 hours a day, 7 days a week, providing convenience for customers to shop at their own pace.
- **Variety of Products and Services:** E-commerce offers a vast array of products and services, ranging from physical goods to digital content, from groceries to travel bookings.
- **Comparison Shopping:** Online platforms facilitate comparison shopping, enabling customers to compare prices, features, and reviews before making a purchase.
- **Personalized Shopping Experiences:** E-commerce websites can gather customer data to personalize shopping experiences, recommending products based on preferences and past purchases

★These business transactions can be done in four ways:

- Business to Business (B2B),
- Business to Customer (B2C),
- Customer to Customer (C2C),
- Customer to Business (C2B).

1. Business to Business

- This is Business to Business transactions. Here the companies are doing business with each other.
- The final consumer is not involved.
- So the online transactions only involve the manufacturers, wholesalers, retailers etc.

2. Business to Consumer

- Here the company will sell their goods and/or services directly to the consumer.
- The consumer can browse their websites and look at products, pictures, read reviews.
- Then they place their order and the company ships the goods directly to them.
- Popular examples are Amazon, Flipkart, Jabong etc.

3. Consumer to Consumer

- Consumer to consumer, where the consumers are in direct contact with each other. No company is involved.
- It helps people sell their personal goods and assets directly to an interested party.
- Usually, goods traded are cars, bikes, electronics etc. OLX, Quikr etc follow this model.

4. Consumer to Business

- This is the reverse of B2C, it is a consumer to business.
- So the consumer provides a good or some service to the company.
- Say for example an IT freelancer who demos and sells his software to a company. This would be a C2B transaction.

Advantages of E-Commerce:

- **Global Reach:** E-commerce allows businesses to reach a global audience, breaking down geographical barriers and expanding their customer base.
- **24/7 Availability:** Online stores are open 24/7, providing customers with the flexibility to shop at any time, which can lead to increased sales and convenience.
- **Lower Operational Costs:** E-commerce businesses often have lower overhead costs compared to brick-and-mortar stores. This includes reduced rent, utilities, and staffing requirements.

Disadvantages of E-Commerce:

- **Security Concerns:** E-commerce is susceptible to security threats, including data breaches, phishing, and cyberattacks that can compromise customer information.
- **Lack of Tangible Experience:** Customers can't physically examine or try products before purchasing, which can lead to dissatisfaction if the product doesn't meet their expectations.
- **Shipping Costs:** High shipping costs, especially for international deliveries, can deter some customers or lead to abandoned shopping carts.

E-contracts:

E-contracts, also known as electronic contracts or cyber contracts, are legally binding agreements formed and executed electronically. They are becoming increasingly common in the modern business world, as they offer several advantages over traditional paper contracts.

- The e-contract takes its legal authority from section 10A of the IT act.
- It says that "Where the **formation of the contract**, offer and acceptance of the contract, as the case may be, are expressed in electronic form, such contract shall not be deemed unenforceable mere on the ground that it was created electronically."
- It means the E-electronic contracts, which follow the essentials of a valid contract and are made electronically, shall be enforceable by law.

Key Benefits of E-contracts

1. **Convenience and Speed:** E-contracts can be executed quickly and easily, without the need for physical signatures or mailing delays.
2. **Cost-Effectiveness:** E-contracts eliminate the need for printing, postage, and storage of paper contracts.
3. **Accessibility:** E-contracts can be accessed and reviewed from anywhere with an internet connection.
4. **Security:** E-contracts can be secured using encryption and other security measures to protect sensitive information.
5. **Environmentally Friendly:** E-contracts reduce the use of paper and other resources, promoting sustainability.

☉ Types of E-contracts

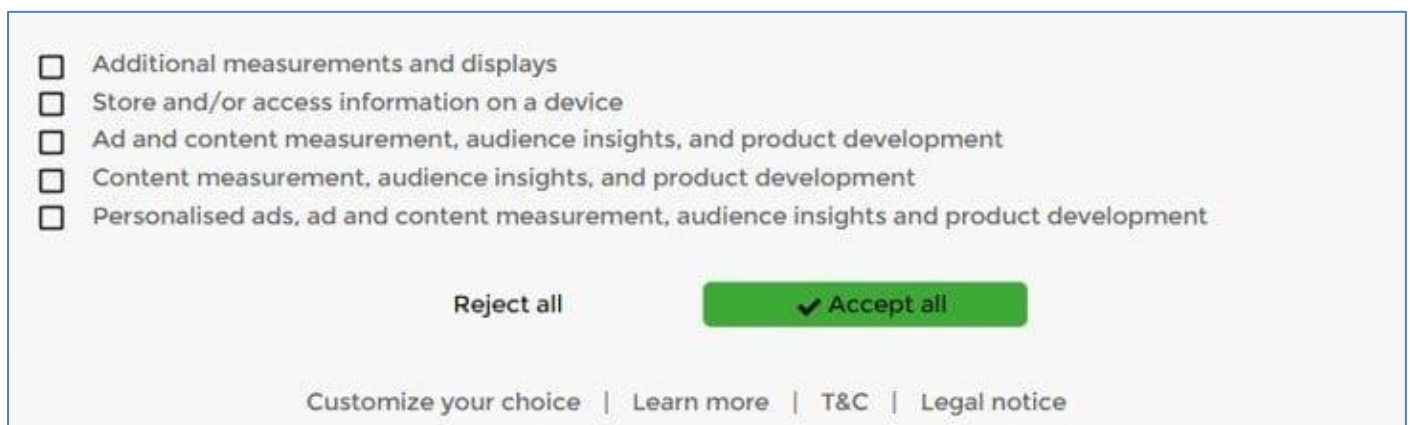
✧ Click-Wrap Agreements

While using any website or any software, we are very familiar with the “I agree” phase, and we press the button without thinking twice. However simple it may appear, it may land us in serious trouble as it gives rise to a legally enforceable valid contract. This type of contract can be legally enforced against the user.

Click-wrap agreements are generally referred to as those agreements or long blocks which nobody reads, these blocks contain terms and conditions of the agreement. But it happens many times that we just click on I agree and continue to the next page.

After clicking on the “I agree” button, it means we accepted all written terms and conditions of the agreement. Such types of agreements are less negotiable and the user has to accept this if he really wants to use that software or any other thing related to this agreement.

For example, you have seen two options: either pay or back while sending the money. Or, while installing software



The screenshot shows a software installation window with a list of permissions. Each item has an unchecked checkbox to its left. Below the list are two buttons: 'Reject all' and 'Accept all' (which is highlighted in green). At the bottom, there are links for 'Customize your choice', 'Learn more', 'T&C', and 'Legal notice'.

- ☐ Additional measurements and displays
- ☐ Store and/or access information on a device
- ☐ Ad and content measurement, audience insights, and product development
- ☐ Content measurement, audience insights, and product development
- ☐ Personalised ads, ad and content measurement, audience insights and product development

[Reject all](#) [✓ Accept all](#)

[Customize your choice](#) | [Learn more](#) | [T&C](#) | [Legal notice](#)

✧ Shrink-Wrap Agreements

Shrink-wrap agreements are mostly related to computer software. The software is mostly distributed in CD-ROMs. When the licensing software is opened by the person for his use, it means he accepts the terms and conditions of that software company.

The term “shrink-wrap” refers to the plastic wrapping which covers the software boxes. This wrapping can be understood as the legally enforceable terms and conditions. As soon as the user removes that wrapping, he is entering into a contract. In simple words, a shrink-wrap agreement is a boilerplate or license agreement containing some terms and conditions packaged with the product. The customer automatically gives his consent when he uses the product.

Following are the terms and conditions which can be made through the Shrink-wrap agreements-

- License
- Fees and payments
- Warranties
- Limitations of liability

✧Browse-wrap agreements

Browse-wrap agreements are probably seen on many websites while searching or reading anything on websites. They are some kind of pop-ups that ask you to click “OK” or “I AGREE” though, you can use the website with or without clicking there.

In this agreement, there is a hyperlink or website containing the terms and conditions over the screen of the website. When the person agrees to the above-stated terms and conditions, he can access the material available and download the product available therein.



Contingent contracts under the Indian Contract Act

Advantages of Contingent Contracts

- It makes the trust between the parties.
- The parties can fix the negotiation before the performance of the contract.
- It helps to reduce the risk of parties.
- The performance of the contract can be cancelled on the happening or non-happening or uncertain event.
- The other party enjoys the benefit if the contract comes into favour.
- It can limit our losses that could happen if the contract fails to fulfil the conditions.

Notice. TermsFeed uses cookies to provide necessary website functionality, improve your experience and analyze our traffic. By using our website, you agree to our [Privacy Policy](#) and our [Cookies Policy](#).

OK

✧Electronic Data Interchange

Electronic Data Interchange means to exchange any type of document of a contract by electronic means.

For example, Exchange of bills by fax.

✧The Security Aspect of Cyber Law:

Electronic data and its transmission are vulnerable to unauthorised interference from criminals and persons having vested interests. Ensuring security of data through legal and technical means has become a matter of concern. A legal infrastructure has become imperative to protect data and information. The gainful use of IT in all walks of life and the development of E-Commerce, hinge to a great extent on the availability and efficacy of the legal infrastructure.

Ernst & Young’s Information Security Survey conducted this year (2000) polled the senior management of companies from all over the world. Altogether, more than 4,300 IT managers from 29 countries responded. The survey found that an overwhelming 82 percent of senior executives now recognise the importance of information security - a significant increase from their first survey five years ago. Security is now viewed as the gateway to new business opportunities, with time out of four respondents indicating that their companies would expand their use of the Internet for business transactions if the security of this medium were improved.

The survey results showed overall agreement on basic information security issues, world-wide. The vast majority of companies say their risks have increased over the past two years, and many organisations have responded by increasing their attention to this area. Most companies employ full-time security professionals, and many have part-time personnel. Only 3 percent have no security function. Despite their heightened awareness of security issues, however, many companies have serious gaps in their security. Twenty percent have not yet adopted a formal security policy. In many organisations that have one, much improvement is required. For example, of the companies that reported a security breach in the past year, only half have taken adequate measures to prevent such incidents in future.

The failure to fully address security issues is reflected in these findings showing that, of the organisations surveyed:

- 36%% do not monitor for network incidents
- 53%%do not monitor their on-line activities (including the Internet)
- 64%% do not have planned incident response

These weaknesses leave security personnel with real problems in responding to security issues. More than half of respondents are not confident that their systems could withstand an internal attack, and more than a third are uneasy about their ability to weather an external assault. Eighty percent of respondents said that winning the commitment of top management is the key to improving their companies' information security. Only 25 percent thought lack of management commitment was actually a barrier. Instead, lack of human resources and employee awareness were noted as the biggest obstacles to improving security.

Data and programs on a stand alone computer or a network of computers can be protected by a procedure called access control. This process allows only authorised people to use the information held on the system. Various access control procedures exist, including the physical locking of the computer. Password protection requires a person to key in a secret arrangement of letters or digits so that computer allows access to the information inside. Some networks have installed a software known as 'firewall', which protects the network from unauthorised external interference.

Data transmitted over a communication link can be protected by being coded. This process is called 'encryption'. A special software carries out the encryption, and encrypted data can be transmitted to other computers through the network. Transmission of encrypted information is insulated against unauthorised interference because the information/data can be decoded only by another computer with the same software.

Cybersecurity law, also known as IT law, addresses the legal issues related to electronic commerce, the use of the internet, and digital technologies. It focuses on protecting individuals, businesses, and organizations from cyber threats and ensuring the security of online activities.

Cybersecurity law is a broad and evolving field, encompassing a wide range of regulations, statutes, and case law. It addresses various cybersecurity concerns, including:

Data Privacy and Protection: Cybersecurity law aims to protect personal data and sensitive information from unauthorized access, use, disclosure, or destruction. It includes regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States.

Cybercrime: Cybersecurity law addresses criminal offenses committed in cyberspace, such as unauthorized access, hacking, data breaches, identity theft, and online fraud. It establishes legal penalties and prosecution guidelines for cybercriminals.

Network Security: Cybersecurity law outlines regulations and guidelines for securing computer networks, systems, and infrastructure to prevent unauthorized access, data breaches, and cyberattacks. It includes standards for network security protocols, encryption, and access controls.

Intellectual Property Protection: Cybersecurity law protects intellectual property rights in the digital realm, addressing issues such as copyright infringement, trademark violations, and unauthorized access to trade secrets.

Cybersecurity Challenges and Considerations

Enforcing cybersecurity law poses unique challenges due to the nature of cybercrime and the complexities of cyberspace:

- **Cross-Border Jurisdiction:** Cybercriminals can operate from anywhere in the world, making it difficult to determine jurisdiction and enforce laws consistently across different countries.
- **Rapid Evolution of Technology:** The ever-evolving nature of technology and cybersecurity threats requires constant adaptation of laws and regulations to stay ahead of emerging risks.
- **Attribution and Proof:** Identifying and attributing cyberattacks to specific individuals or groups can be challenging, making it difficult to prosecute cybercriminals effectively.
- **International Cooperation:** Effective cybersecurity requires international cooperation and collaboration among law enforcement agencies and governments to share intelligence and combat cybercrime effectively.

Cybersecurity Law and the Future:

Cybersecurity law will continue to play a crucial role in protecting individuals, businesses, and organizations from cyber threats as technology advances and the digital world becomes increasingly interconnected. As we move forward, it is essential to:

- **Regularly Review and Update Laws:** Cybersecurity laws need to be regularly reviewed and updated to keep pace with the evolving threats and technologies in the digital realm.
- **Enhance International Collaboration:** International cooperation and collaboration among law enforcement agencies and governments are essential for effectively combating cybercrime and protecting digital assets worldwide.
- **Promote Cybersecurity Awareness:** Public awareness and education about cybersecurity threats and best practices are crucial for minimizing risks and protecting individuals and organizations from falling victim to cyberattacks.

The Intellectual Property Aspect in Cyber Law:

Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium.

The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO) –

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic, and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms, and broadcasts
- Trademarks, service marks, commercial names, and designations
- All other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields

Copyright

- Copyright is a right given by the law to creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings. Unlike the case with patents, copyright protects the expressions and not the ideas.

...the Concept of Cyberspace)...Page No. (4-20)

- There is no copyright in an idea. Just as you would want to protect anything that you own, creators want to protect their works. Copyright ensures certain minimum safeguards of the rights of authors over their creations, thereby protecting and rewarding creativity.
 - Under section 13 of the Copyright Act, 1957, Copyright protects above discussed creativity of inventors. Creativity being the keystone of progress, no civilized society can afford to ignore the basic requirement of encouraging the same.
- Economic and social development

Patent

- Patents are rights under Intellectual Property Rights related to an invention for which patent has been given by the Government/statute to the patentee in exchange of full disclosure of their invention either an individual or a company/organization.
- Patent has been given as exclusive right for a limited period to exclude others from making, using, selling and importing the patented product or process producing that product. The patent rights are enjoyable without any insight to the invention place, field of technology and the products either imported or produced locally.

In India, the law relating to Patents is contained in the Patents Act, 1970. This Act has been amended in the years 1995, 1999, 2002 and 2005 respectively to meet the challenges of changing times and also to meet India's obligations under the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) which forms a part of the Agreement establishing the World Trade Organization (WTO).

Database rights

- Copyright is legal device that gives the owner the right to control how a creative work is used. Until several years ago the contents of a database could not be legally protected. Producers of databases that contained factual data could not claim copyright protection which made it impossible for them to prevent others from copying content.
- A database is defined in the directive as "a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means."

- Database rights specifically protect this effort and investment. Investment includes "any investment, whether of financial, human or technical resources" and substantial means "substantial in terms of quantity or quality or a combination of both".
- Metadata will be included in this investment.

- Databases are treated as a class of literary works and may also be given copyright protection for the selection and/or arrangement of the contents under the terms of the Copyright, Designs and Patents Act 1988.

Design Rights

- An industrial design right is an intellectual property right that protects the visual design of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or colour, or combination of pattern and colour in three-dimensional form containing aesthetic value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft.
- The registration and protection of industrial designs in India is administered by the Designs Act, 2000 and corresponding Designs Rules, 2001 which came into force on 11th May 2001 repealing the earlier Act of 1911.
- The Design Rules, 2001 was further amended by Designs (Amendment) Rules 2008 and Designs (Amendment) Rules 2014. The last amendment in Designs Rules came in to force from 30th December, 2014, which incorporates a new category of applicant as small entity in addition to natural person and other than small entity.

Trademarks

- A trademark can be composed of logos, images, words, short phrases, colours or even a compound of all of these. The most commonly used are words and pictures however, other distinguishable marks may also be used if they are capable of graphical representation.
- For instance Louis Vuitton, the famous luxury brand has obtained a trademark for its check pattern which is known as the Damier Pattern, the infamous confectionery brand Cadbury has the colour purple trademarked for its chocolates even though trademark for a single colour is very hard to obtain. And Coca-Cola has a trademark for its bottle's design. Some more examples of trademarks are DETTOL, ROLEX, NESTLE, SUN PHARMA, THEOBROMA, MONT BLANC etc.

- A trademarked name marks all of the products and services as the proprietor's and no one else's and also prevents loss of reputation due to counterfeit products. A Trademark is valid for 10 years and it can be renewed indefinitely on payment of additional fees. Trademark rights are private rights and protection is enforced through court orders.
- In India, the Trade Marks Act, 1999 deals with several aspects of trademarks like registration, protection, provisions of relief in case of infringement etc. India is a signatory of the Paris convention and the TRIPS agreement and hence the Act is compliant with the principles thereof.

Advantages of Intellectual Property Rights

- It provides exclusive rights to the creator's or inventor's.
- It gives freedom to inventor to share his knowledge without keeping its secret.
- It helps to creator financially.
- It provides legal defence to the creator

The Evidence Aspect in Cyber Law:

- The evidence is the important function of the trial court. With the growth of the e-commerce the electronic evidences have come in picture. Admissibility of electronic evidence, proving digital signature, relevance of proof is important before giving the verdict. Provisions related to evidence are given in Indian Evidence Act, 1872.
- Now a day's Electronic agreements, electronic messages, and digital signatures are making a great impact on our lives. It is a general perception that electronic evidence is not covered in Indian Evidence Act, 1872. The Indian Evidence Act, 1872 is amended by the IT Act, 2000.
- Let's see the status of computer records or electronic records in the Indian Evidence Act 1872 before and after the IT Act 2000.

The Section 3 mentions the definition of evidence, proved and the fact.

- 1 **Evidence:** In evidence act the evidence are oral evidences that is statements of the witness and documentary evidences The two types of evidences recognized by the definition of evidence are oral

evidence and documentary evidence. The definitions of facts and proved gives things and object status of evidences.

2. **Proved** : A fact is said to be proved when, after considering the matters before it, the Court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists.

3. **Facts** : It includes things or objects.

Types of Digital Evidence

Digital evidence encompasses a wide range of electronic information that can be used to prove or disprove a fact in a cybercrime case. Common types of digital evidence include:

- **Electronic Records**: These include digital documents, emails, chat logs, social media posts, and website content.
- **Computer System Data**: This comprises data stored on hard drives, memory cards, and other storage devices, including operating system files, application data, and user activity logs.
- **Network Traffic Data**: This encompasses data packets exchanged over computer networks, providing insights into network activity, communication patterns, and potential cyberattacks.
- **Mobile Device Data**: This includes data stored on smartphones, tablets, and other mobile devices, such as call logs, text messages, location data, and app usage data.

The following are some provisions of the Indian evidence Act, 1872 which are altered in IT Act, 2000.

- In Section 17 of the Indian evidence Act, 1872, for the words "oral or documentary," words "oral or documentary or contained in electronic form" shall be substituted by IT Act, 2000.
- In Section 34 of the Indian evidence Act, 1872, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted by IT Act, 2000.
- In Section 35 of the Indian evidence Act, 1872, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted by IT Act, 2000.
- In Section 59 of the Indian evidence Act, 1872, for the words "contents of documents "the words" contents of documents or electronic records" shall be substituted by IT Act, 2000.
- Section 39 of the Indian evidence Act, 1872 is substituted vide the IT Act, 2000.
- "Section 39 What evidence to be given when statement forms part of a conversation, documents, electronic record, book or series of letters or papers.

Global Trends in Cyber Law :

Global trends in cyber law are constantly evolving as technology advances and new threats emerge. Some of the key trends in cyber law in 2023 include:

The increasing importance of data protection and privacy: Data breaches and cyberattacks are becoming more common and sophisticated, and there is a growing global consensus on the need for stronger data protection and privacy laws. The General Data Protection Regulation (GDPR) in the European Union is a leading example of such legislation, and other countries are developing their own data protection laws.

The rise of ransomware: Ransomware is a type of malware that encrypts an organization's data and demands a ransom payment in exchange for the decryption key. Ransomware attacks have become increasingly common and costly, and governments are working to develop effective strategies to combat this threat.

The growing sophistication of cyberattacks: Cybercriminals are using increasingly sophisticated techniques to attack computer systems and networks. This includes using artificial intelligence and machine learning to automate attacks and evade detection.

The challenges of cross-border cybercrime: Cybercrime is a global problem, and it can be difficult to investigate and prosecute cybercriminals who operate across borders. Governments and law enforcement agencies are working to develop international cooperation mechanisms to combat cross-border cybercrime.

The need for cybersecurity awareness and education: Cybersecurity awareness and education are essential to protect individuals and organizations from cyberattacks. Governments, businesses, and schools are all working to raise awareness of cybersecurity risks and best practices.

The increasing role of artificial intelligence in cybersecurity: Artificial intelligence (AI) is playing an increasingly important role in cybersecurity. AI can be used to detect and respond to cyberattacks, automate security tasks, and develop new security solutions.

Legal Framework for Electronic Data Interchange Law Relating to Electronic Banking

4.8.1 Introduction : Definition and Concept

GQ. What is EDI? Explain its relevance to companies.

GQ. Write note on Electronic Data Interchange Scenario in India.

EDI (Electronic Data Interchange) can be defined as the exchange of documents in standardized electronic form, between organisations in an automated manner, directly from a computer application in one organisation to an application in another.

It can also be defined as computer-to-computer exchange of structured data, sent in the form that allows for automatic processing with no manual intervention.

According to the UNCITRAL definition, "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information.

The type of documents exchanged by EDI includes business transactions such as orders, invoices, and delivery advice and payment instructions as a part of EFT (electronic funds transfer).

There are 2 key elements in basic EDI. Firstly, electronic documents replace their paper counterparts. Secondly, the exchange of documents takes place in a standardized format.

In a typical EDI application to support purchasing, an EDI system is integrated with the existing purchasing system at the customer side.

When a customer enters a new purchase request into the purchasing system, a corresponding request is received by the sender's EDI system, which then constructs an electronic purchase order document and transmits it to the supplying company.

Originally, all EDI transactions were sent over dedicated communication channels, which meant that such channels had to be set up between any pair of organizations wishing to use EDI between themselves.

The Electronic Data Interchange Scenario in India

The Ministry of Commerce is the nodal agency for the implementation of electronic data Interchange (EDI) in India. India joined the EDI movement in early 1992, when it obtained the observer status in the Asia EDIFACT Board (ASEB). India became a member of ASEB in August 1992. In order to promote the use of EDI in India the Ministry of Commerce has taken initiatives to develop EDI infrastructure. The following are the agencies that cater to the EDI infrastructure.

- | | |
|---|----------------------------|
| 1. EDI Council of India | 2. India EDIFACT Committee |
| 3. Working Group | 4. Education and Awareness |
| 5. VAN Service Providers | |
| 6. EDI Implementation in Government Regulatory Agencies | |

(1) EDI Council of India

EDI council is the apex body consisting of all the key government departments and representatives of trade and industry. It is responsible for laying down the policy frame work and direction for-

- promotion and propagation of EDI and Electronic Commerce.
- creating awareness and education among the potential EDI functionaries and users
- streamlining procedures and practices
- attending to legal issues
- human resource development
- any other issue connected with EDI and Electronic Commerce.

Chairman : Secretary, Ministry of Commerce

Secretariat : EDI Division

Ministry of Commerce

Udyog Bhawan,

New Delhi – 1100011

► (2) India EDIF ACT Committee

The India EDIFACT Committee (IEC) is responsible for formulating standards, streamlining the procedures in line with UN/EDIFACT and maintain liaison with UN/EDIFACT bodies.

To address all the information needed on different sectors and its interface with UN/EDIFACT standards following Message Development Groups are working-

- Ports Message Development Group under Indian Ports Association (IPA)
- Airports Message Development Group under Airports Authority of India (AAI)
- Financial Message Development Group under Indian Banks Association (EBA)
- Customs Message Development Group under Central Board of Excise and Custom (CBEC)

Chairman : Additional Secretary, Ministry of Commerce

(MU-New Syllabus w.e.f academic year 22-23)(M7-153)



Tech-Neo Publications...A SACHIN SHAH Venture

Cyber Security and Laws (MU - Sem. 7)

(The Concept of Cyberspace)...Page No. (4-3)

Secretariat : EDI Division

Ministry of Commerce

Udyog Bhawan,

New Delhi-1100011

► (3) Working Group

The working group is responsible for motivating various functionaries in the government and ensure scheduled implementation of program.

Chairman : Secretary, Ministry of Commerce

Secretariat : EDI Division

Ministry of Commerce

Udyog Bhawan,

New Delhi - 1100011

► (4) Education and Awareness

- Federation of Indian Export Organisations (FIEO) is organising regular workshops and seminars throughout in India. FIEO has identified large automotive, chemical, textile and engineering concerns that had already implemented EDI. These Organisations would perform as model organisation for the EDI implementation in their own sectors.

- The All India Management Association (ALMA) of New Delhi is offering courses on EDI, including a Masters program. An HRD group is also working to investigate the needs for EDI related human resource development.

► (5) VAN Service Providers

- The two major VAN operators in India providing EDI services are NIC and VSNL.
- National Informatics Center (NIC) has set up a nation-wide computer communication network with over 600 nodes connecting the national capital, the state capitals and district headquarters. NICNET provides high speed information highway nodes within the country and connectivity to Internet as well as to other foreign networks outside the country.

4.8.3 Benefits of EDI

EDI was developed to solve the problems inherent in paper-based transaction processing and in other forms of electronic communication. In solving these problems, EDI is a tool that enables organizations to reengineer information flows and business processes. It directly addresses several problems long associated with paper-based transaction systems :

- (1) **Time delays** : Paper documents may take days to transport from one location to another, while manual processing methodologies necessitate steps like keying and filing that are rendered unnecessary through EDI.
- (2) **Labor costs** : In non-EDI systems, manual processing is required for data keying, document storage and retrieval, sorting, matching, reconciling, envelope stuffing, stamping, signing, etc. While automated equipment can help with some of these processes, most managers will agree that labor costs for document processing represent a significant proportion of their overhead. In general, labor-based processes are much more expensive in the long term than are EDI alternatives.
- (3) **Accuracy** : EDI systems are more accurate than their manual processing counterparts because there are fewer points at which errors can be introduced into the system.
- (4) **Information Access** : EDI systems permit myriad users access to a vast amount of detailed transaction data in a timely fashion. In a non-EDI environment, in which information is held in offices and file cabinets, such dissemination of information is possible only with great effort, and it cannot hope to match an EDI system's timeliness. Because EDI data is already in computer-retrievable form, it is subject to

4.9.1 Law Relating to Electronic Banking

GQ. What are the different laws for e-banking?

GQ. Explain different services provide to internet banking.

- Electronic banking is a service allowing an account holder to obtain account information and manage certain banking transactions through a personal computer. The service is provided through the bank's web site on the internet. In electronic banking, funds are transferred through an exchange of electronic signals. The transfer is recorded on computer systems connected by telephone lines. Instead of through a check or signature, identification is made through passwords.
- E-banking is being used in India for some time now in the form of digital data in computers, credit and debit cards, Automated Teller Machines, Mobile Banking, net banking and internet banking. Internet or e-banking means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions.
- E-banking has been defined in law lexicon as banking activities accessed by using a computer, employing modems and telephones.
- In e-banking, 'e' stands for electronic and the banking has been defined as 'an acceptance of money from the public, for purpose of lending or investment of money, which is withdrawable by cheque, draft or otherwise' and banking by using electronic devices is e-banking.

4.9.2 Services of e-banking Includes

- (1) **Information System :** General Information like interest rates, branch location, bank products and their features, loan and deposit features are provided in the bank website. There exist facilities for downloading various types of application forms like deposit application form, loan application form, etc. The communication is carried through e-mail, otherwise the person seeking information need not disclose his identity. Also, there is no possibility of any unauthorized person getting into production systems of the bank through internet.
- (2) **Electronic Information Transfer System :** The system provides customer with specific information in the form of account balances, transaction details and statement of accounts. The information is still largely of the 'read only' format.

Electronic Clearing System (ECS):

Electronic Clearing System (ECS) is an electronic method of fund transfer from one bank account to another. It is generally used for bulk transfers performed by institutions for making payments like dividend, interest, salary, pension, etc. ECS can also be used to pay bills and other charges such as payments to utility companies such as telephone, electricity, water, or for making equated monthly installments payments on loans as well as SIP investments.

a. ECS credit – ECS credit is used for allowing credit to a large number of beneficiaries by raising a single debit to the customer's account, such as dividend, interest or salary payment. ECS payments can be performed by any institution (ECS user) that has to make bulk or repetitive payments to a number of recipients or beneficiaries. They initiate the transactions after registering themselves with an approved clearinghouse. ECS users also have to obtain a consent such as the account particulars of the beneficiaries for engaging in the ECS clearings. – Under the scheme, the beneficiaries of the repetitive or regular payments can also require the paying institution to make ECS (credit) for payment. The ECS users expect to effect payments and to present the data in a prescribed format to any one of the recognized clearinghouses. The clearinghouse will debit the account of the ECS user through the user's bank on a particular day and credit the accounts of the recipient banks, for providing onward credit to the accounts of the ultimate beneficiaries. The benefits of ECS credit given to the clients are as follows :

- The end beneficiary need not make frequent visit to his bank for depositing the physical paper instruments.
- Delay in the realization of proceeds, which used to happen in the receipt of the paper instrument is eliminated. o The ECS user helps to save on administrative machinery for printing, dispatch and reconciliation.
- Provides the ability to make payment and ensure that the beneficiaries account gets credited on a designated date.

B ECS debit

– ECS debit is used for raising debits to a number of accounts of consumers or account holders for affording a single credit to a particular institution, in cases such as utility payments like electricity bills and telephone bills. ECS debit is a scheme in which an account holder can authorise an ECS user to recover a prescribed amount by raising a debit on his account. The ECS user has to receive an authorisation which is called ECS mandate for raising such debts. These mandates have to be approved by the bank branch maintaining the account.

– Any ECS user participating in the scheme has to register with an approved clearinghouse, an ECS user should receive the mandate forms from the participating destination account holders with the bank's acknowledgement. A certified copy of the mandate should be available with the drawee bank.

– The ECS user has to submit the data in a specified form through the sponsor bank to the clearinghouse. The clearinghouse would pass on the debit to the destination account holder through the clearing system and credit the sponsor bank's account for onward crediting the ECS user. All the unprocessed debits have to be returned to the sponsor bank's account for onward crediting the ECS user. All the unprocessed debits have to be returned to the sponsor bank, within the time frame specified. Banks treat the electronic instructions received through the clearing system at par with the physical cheques. The benefits of ECS debit given to the clients are as follows :

- Trouble-free: Eliminates the need to go to the collection centres or banks and the need to stand in long queues for payment. Cyber Security and Laws (MU-Sem 7) 4-41 The Concept of Cyberspace
- Easy to track: Customers are not required to track down payments by last dates. The ECS users would monitor the debts. The ECS user saves on administrative machinery for collecting the cheques by monitoring their realisation and reconciliation.
- Better cash management: Chances of frauds due to fraudulent access to paper instruments and encashment are avoided. o The realisation of payments on a single date is enabled instead of fractured receipt of payments.

4.9.3 Law Relating to E-Banking in India

Law relating to banking in India has undergone sweeping changes after the advent of technology. The changes have been made due to revolution in banking sector worldwide. To meet the international standard in service the transformation was necessary. There are amendments carried to the existing laws to meet the needs of the technology in banking.

(1) Reserve Bank of India Act, 1934

- In 1995, the Reserve Bank had set up the Committee for Proposing Legislation on Electronic Funds Transfer and other Electronic Payments. Based on the recommendation, the Reserve Bank of India Act, 1934 (herein after referred as RBI Act, 1934) was amended to include electronic banking operation.

MU-New Syllabus w.e.f academic year 22-23)(M7-153)



Tech-Neo Publications...A SACHIN SHAH Venture

- A new clause to section 58, sub-section 2 of the Act, relating to the regulation of funds transfer through electronic means between banks, i.e. transactions like Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) and other funds transfer was inserted, to facilitate such EFTs and ensure legal admissibility of documents and records.

(2) Banking Regulation Act, 1949

The Act originally came into force on 16th March, 1949 and it was known as Banking Companies Act, 1949. It was amended and renamed as Banking (Acquisition and Transfer of Undertaking) Act, 1969 and the original Act was extended to the cooperative banks from 1966 and is simply called as B.R. Act, 1949. The objectives of the Act are, to safeguard the interest of depositors, to develop banking institutions on sound lines and to attain the monetary and credit system to the larger interests and priorities of the nation.

(3) Negotiable Instruments Act, 1881

- Under the Negotiable Instruments Act, 1881, cheque includes electronic image of truncated cheque and a cheque in the electronic form.
- The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Cheque truncation, loosely defined, is the process in which the physical movement of

(MU-New Syllabus w.e.f academic year 22-23)(M7-153)



Tech-Neo Publications...A SACHIN SHAH Venture

Cyber Security and Laws (MU - Sem. 7)

(The Concept of Cyberspace)...Page No. (4-46)

cheque within bank, between banks and clearing house is curtailed or eliminated, being replaced in whole or in part, by electronic records of their content, with or without images, for further processing and transmission. The truncation of cheque in clearing house...

(5) Prevention of Money Laundering Act, 2002

- Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy.
- Money laundering is defined as the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime.
- In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income.

implement protocols before the criminal behaviour occurs.

(6) Information Technology Act, 2000

- This is the pivotal legislation dealing with crimes committed due to technology in India. Technological innovation in general and IT applications in particular, have had a major effect in banking and finance.
- The technology and security standards are of prime importance as the entire base of Internet banking rests on it. If the technology and security standards are inadequate, then Internet banking will not provide the desired results and will collapse ultimately.

7) The Payment and Settlement Systems Act, 2007

- It is internationally acknowledged that payment and settlement systems should function on a well-founded legal basis. This entails among other things, proper authorization requirement for setting up and payment systems, legal recognition for netting, settlement finality, providing for regulation and oversight of the payment and settlement systems.
- In India there is no enactment which dealt with the issue of Electronic Fund Transfer (EFT). The Payment and Settlement Act (herein referred as PSS Act) and the directions and guidelines issued there under deal, to a certain extent, with the issue.
- In order to strengthen the institutional framework for the payment and settlement systems in the country, the RBI constituted, in 2005, a Board for Regulation and Supervision of Payment and Settlement Systems as a Committee of its Central Board. The Board which was chaired by the Governor of RBI, while all the four Deputy Governors and two external Directors of the Central Board are its members.

The Need for an Indian Cyber Law:

4.10 THE NEED FOR AN INDIAN CYBER LAW

GQ. Why there is need of Cyber law? Explain.

In the present world which is more tech-savvy, the words cyber law and cyber crimes have also become more sophisticated. Internet and technology were launched for research purposes and making the lives of humans easy but as the use and number of people on the internet increased, the need for cyber laws in India was felt. As the nature of the internet is anonymous it is easy to commit cybercrimes. Thereby many could misuse this aspect largely.

With the evolution and development of the internet, information technology and computers, challenges imposed by cyber crimes have also increased. Therefore, cyber laws regulate all fields of laws in which cyber crimes can be committed, such as criminal law, contract, intellectual property law and tort. Cyber laws deal with various kinds of concerns, such as free speech, safety, intellectual property rights, privacy, terrorism, e-commerce and jurisdiction of cyber laws.

A comprehensive cyber law for India is essential for several reasons:

1. Protecting Individuals and Organizations from Cybercrime

Cybercrime, encompassing offenses such as hacking, data breaches, identity theft, and online fraud, has become a significant threat to individuals, businesses, and organizations in India. A comprehensive cyber law would provide a robust legal framework for preventing, investigating, and prosecuting cybercrimes, safeguarding the interests of citizens and businesses.

2. Regulating Cyberspace and Electronic Commerce

The growth of e-commerce, online transactions, and digital services necessitates clear regulations to ensure fair competition, protect consumer rights, and promote responsible use of cyberspace. A comprehensive cyber law would establish a legal framework for regulating cyberspace activities, promoting responsible digital behavior, and fostering a trusted and secure online environment.

3. Addressing National Security Concerns

Cyberattacks pose significant threats to national security, potentially disrupting critical infrastructure, compromising sensitive information, and undermining national stability. A comprehensive cyber law would empower the government to protect critical infrastructure, defend against cyberattacks, and establish clear guidelines for cybersecurity measures.

4. Advancing India's Digital Transformation

India's digital transformation agenda is crucial for economic growth and social progress. A comprehensive cyber law would create a supportive legal environment for innovation, investment, and adoption of digital technologies, fostering a vibrant and secure digital economy.

5. Harmonizing with International Standards

India participates in various international forums and agreements related to cybercrime and cybersecurity. A comprehensive cyber law would align India's legal framework with international standards, facilitating cooperation with other countries in combating cyber threats and promoting responsible cyberspace activities.