SINCE 1999
SYNERGY
A Modern Day Gurukul

SYNERGY INSTITUTE OF ENGINEERING & TECHNOLOGY
Department of Computer Science & Engineering
Academic Session 2023-24
LECTURE NOTE

Name of Faculty	: Mr. SMRUTI RANJAN DASH
Name of Subject	: CYBER LAW & ETHICS
Subject Code	: RCL7E004
Subject Credit	: 3
Semester	: VII
Year	: 4th
Course	: B.TECH
Branch	: COMPUTER SCIENCE & ENGINEERING
Admission Batch	: 2020-24

UNIT -1

Introduction to Cyber Law

How Computers Evolved?

Computers in the form of personal desktop computers, laptops and tablets have become such an important part of everyday living that it can be difficult to remember a time when they did not exist. In reality, computers as they are known and used today are still relatively new. Although computers have technically been in use since the abacus approximately 5000 years ago, it is modern computers that have had the greatest and most profound effect on society. The first full-sized digital computer in history was developed in 1944. Called the Mark I, this computer was used only for calculations and weighed five tons. Despite its size and limited ability it was the first of many that would start off generations of computer development and growth.

First Generation Computers

First generation computers bore little resemblance to computers of today, either in appearance or performance. The first generation of computers took place from 1940 to 1956 and was extremely large in size. The inner workings of the computers at that time were unsophisticated. These early machines required magnetic drums for memory and vacuum tubes that worked as switches and amplifiers. It was the vacuum tubes that were mainly responsible for the large size of the machines and the massive amounts of heat that they released. These computers produced so much heat that they regularly

overheated despite large cooling units. First generation computers also used a very basic programming language that is referred to as machine language.

Second Generation Computers

The second generation (from 1956 to 1963) of computers managed to do away with vacuum tubes in lieu of transistors. This allowed them to use less electricity and generate less heat. Second generation computers were also significantly faster than their predecessors. Another significant change was in the size of the computers, which were smaller. Transistor computers also developed core memory which they used alongside magnetic storage.

Third Generation Computers

From 1964 to 1971 computers went through a significant change in terms of speed, courtesy of integrated circuits. Integrated circuits, or semiconductor chips, were large numbers of miniature transistors packed on silicon chips. This not only increased the speed of computers but also made them smaller, more powerful, and less expensive. In addition, instead of the punch cards and the printouts of

previous systems, keyboards and monitors were now allowing people to interact with computing machines.

Fourth Generation Computers

The changes with the greatest impact occurred in the years from 1971 to 2010. During this time technology developed to a point where manufacturers could place millions of transistors on a single circuit chip. This was called monolithic integrated circuit technology. It also heralded the invention of the Intel 4004 chip which was the first microprocessor to become commercially available in 1971. This invention led to the dawn of the personal computer industry. By the mid-70s, personal computers such as the Altair 8800 became available to the public in the form of kits and required assembly. By the late 70s and early 80s assembled personal computers for home use, such as the Commodore Pet, Apple II and the first IBM computer, were making their way onto the market. Personal computers and their ability to create networks eventually would lead to the Internet in the early 1990s. The fourth generation of computers also saw the creation of even smaller computers including laptops and hand-held devices. Graphical user interface, or GUI, was also invented during this time. Computer memory and storage also went

through major improvements, with an increase in storage capacity and speed.

The Fifth Generation of Computers

In the future, computer users can expect even faster and more advanced computer technology. Computers continue to develop into advanced forms of technology. Fifth generation computing has yet to be truly defined, as there are numerous paths that technology is taking toward the future of computer development. For instance, research is ongoing in the fields of nanotechnology, artificial intelligence, as well as quantum computation.

Emergence of cyber space

cyberspace, amorphous, supposedly “virtual” world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet’s infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state.

The term *cyberspace* was first used by the American-Canadian author William Gibson in 1982 in a story published

in *Omni* magazine and then in his book *Neuromancer*. In this science-fiction novel, Gibson described cyberspace as the creation of a computer network in a world filled with artificially intelligent beings.

……..

Cyber Jurisprudence

Introduction

Jurisprudence can be defined as the science and philosophy or theory of the law. Applying jurisprudence to cyber law gives rise to the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law. Cyberlaw is a very recent concept and if compared with other older branches of the law, is a little structured study.

The term cyberspace was originally coined by a science fiction writer William Gibson to depict data matrices existing in a dark distant future which means the information spaces made by the technology of digital networked computer systems that ultimately connect with the mother of all networks that is the Internet. With the advent of the internet and technology, cyberspace along with a number of crimes related to the same emerged and expanded. As we enter the cyber age, the law on all fronts is struggling to keep pace with technological advances in cyberspace. While there is a prosperous discussion of the nature of cyber law and its challenges, still a

fundamental body of scholarly contributions to the discussion is lacking. The outgrowth of cyber jurisprudence around the world has promoted the emergence of newer dimensions in Law. The focus is on the practical aspect of cybercrime with the initial attempt to extend the known physical society concepts to the virtual space rather than the theory, philosophy, and science of cyberlaw generally. Hence in due course, we need to develop separate Cyber Jurisprudence to deal with future disputes.

The modern jurists have been cautious to endow with the rationale pedestal of jurisprudence to this ruling and now ascertained utmost exact definition of cyber jurisprudence as this describes the principles of legal issues, which exclusively

regulates the cyberspace and internet can be termed as cyber jurisprudence with a virtual approach.

Jurisprudential Aspects of Cyber Laws

Cyber jurisprudence gives an analysis of the land with land and no border, different from the physical world, they may be virtual from origin and nature. This covers the virtual world with virtual rules and policies, along with the virtual subject matter, virtual contracts, virtual disputes, virtual property, virtual possession, and virtual court.

The existence of an item in the context of a virtual world, such as an e-mail account or an online game, is also a form of virtual property. It emphasizes the composite idea of cyber jurisdiction, cyber court's venue in the cyberspace, and recognize uniform cyber rules and policies at the international level. Framing rules and laws to cover every aspect will be an arduous task since the cyber world has no boundaries.

However, a balance has to be maintained and laws be evolved in order to keep a check on cybercrimes. Whenever a conflict is encountered in implementing existing laws of the real space to Cyber Space, the laws of the real space have prevailed, overtime this tendency is likely to develop into a principle of "Primacy of Meta Space" and become the bedrock of Jurisprudence. However, the principle fails when two laws of the real space itself come into conflict in the Cyber Space.

Doctrinal approach

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.
IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

According to the Ministry of Electronics and Information Technology, Government of India :

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crime

Importance of Cyber Law:

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud*:**
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. ***Copyright*:**
   The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.

3. ***Defamation*:**
   Several personnel uses the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

4. ***Harassment and Stalking*:**
   Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

5. ***Freedom of Speech*:**
   Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allows people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. ***Trade Secrets*:**
   Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade secrets.

7. ***Contracts and Employment Law*:**
   Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Consensual approach

A consensual definition allows future research to be aligned and it facilitates the interpretation and comparison of existing research. The findings suggest that the routine activity approach can be applied to the digital world

Cyber Ethics

cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have defined policies about cyberethics.

In the late 19th century, the invention of cameras spurred similar ethical debates as the internet does today. During a seminar of *Harvard Law Review* in 1890, Warren and Brandeis defined privacy from an ethical and moral point of view to be:

> "central to dignity and individuality and boyhood. Privacy is also indispensable to a sense of autonomy — to 'a feeling that there is an area of an individual's life that is totally under his or her control, an area that is free from outside intrusion.' The deprivation of privacy can even endanger a person's health."

Over 100 years later, the internet and proliferation of private data through governments and ecommerce is an area which requires a new round of ethical debate involving a person's privacy.

Privacy can be decomposed to the limitation of others' access to an individual with "three elements of secrecy, anonymity, and

solitude." Anonymity refers to the individual's right to protection from undesired attention. Solitude refers to the lack of physical proximity of an individual to others. Secrecy refers to the protection of personalized information from being freely distributed.

Individuals surrender private information when conducting transactions and registering for services. Ethical business practice protects the privacy of their customers by securing information which may contribute to the loss of secrecy, anonymity, and solitude. Credit card information, social security numbers, phone numbers, mothers' maiden names, addresses and phone numbers freely collected and shared over the internet may lead to a loss of Privacy.

Fraud and impersonation are some of the malicious activities that occur due to the direct or indirect abuse of private information. Identity theft is rising rapidly due to the availability of private information in the internet. For instance, seven million Americans fell victim to identity theft in 2002, and nearly 12 million Americans were victims of identity theft in 2011 making it the fastest growing crime in the United States.[1] Public records search engines and databases are the main culprits contributing to the rise of cybercrime. Listed below are a few recommendations to restrict online databases from proliferating sensitive personnel information.

1. Exclude sensitive unique identifiers from database records such as social security numbers, birth dates, hometown and mothers' maiden names.
2. Exclude phone numbers that are normally unlisted.
3. Clear provision of a method which allows people to have their names removed from a database.
4. Banning the reverse social security number lookup services.

Cyber Jurisdiction

A fast-paced world, and surprisingly fitting in one's hand. The world is in the era of "internet and cyberspace", and it seems faster and better than ever. But it all comes with a price, that mankind is still in the exploration of. Just as in the real and physical world, the virtual space created by humans also sees a plethora of criminal activities on a day to day basis where the data of millions of people acts as valuable assets. It has the power to instigate a civil war or to destroy nations altogether, steal data for ransom, or even rob millions from a bank in seconds. It becomes quite a challenge to map out a conclusive set of applicable laws to contain this mass virtual force. The major obstacle being how, when these offences are prosecuted, the personal jurisdiction is to be applied.

This article breaks down how the legal principles have evolved while determining personal jurisdiction in cyberspace.

Cyberspace- The Virtual Universe

Cyberspace is an imaginary area or a virtual space where a connection can be established between two computers at any two points in the world, with absolutely no limits.

The word 'cyberspace' was used in the Novel **'Neuromancer' by William Gibson**, for the first time in 1984, which is a science fiction and defined as an interaction between the human mind and computers. 1

While cyberspace and the internet share very similar connotations, cyberspace can be defined as anything that is done using the internet, while the internet is a network or networks.

In layman terms "cyberspace" is a virtual universe made up of the widely spread and interconnected digital gadgets and technology, enabling one to create, modify, share, exchange, extract and destroy the physical resources floating all over the internet.

The world we live in is possibly at its simplest, most sophisticated version, as at this point in time, and we could only hope for it to make many innovative new changes. The world seems so much smaller at our fingertips, lives have collectively become easier. Education, E-commerce, shopping, banking, and almost every other essential has taken its spot on the internet. In fact, some of the richest multinational companies are that of Google and Facebook that are empires built virtually on nothing but data. The huge number of users are the customers and their personal information, the asset. Each of these businesses run on nothing but loads of information, some private, some not, and it becomes necessary to build a hyper-vigilant screening process in providing our personal information, because of the immense threats that tag-along with this mighty tool.

With business transactions moving online, the conventional methods of dealing with legal complications are also in need of remoulding to fit into the present, needful circumstances.

It is often very ambiguous to decipher what place holds jurisdiction over disputes that arise in the vast cyberspace. In her paper "Principles of Jurisdiction", Betsy Rosenblatt states that "a court must first decide "where" the internet conduct takes place, and what it means for internet activity to have an "effect" within a state or a nation".

The concept of national borders and distance stands irrelevant in cyberspace. By setting up a website from a home computer, here in India, one can grant access to anybody around the world, making communication a piece of cake. While communication is easier, the legal threats posed are quite drastic.

Threats To Cyberspace

With the amount of information being constantly exchanged, the threats in cyberspace are equally large. It is also important to register the intensity of changes the cyberspace is constantly subjected to, which concurrently aids in the advancement of the cyberattacks.

Cyberattacks can range from personal data breaches to mass frauds, each of which is equally dangerous and harmful, putting one's usage of cyberspace at risk.

Cyberattacks are where internet users use malicious maneuvres to steal, destroy, expose, or gain unauthorized access into the personal information of a person, company, military databases, etc.,

Cyberattacks are a part of cyber warfare- where cyberspaces containing classifies military information, are attacked to wage war and other military purposes, and cyber terrorism- where cyberspaces are used to conduct violent criminal activities.

Some of these common cyberattacks include phishing, identity theft, ransomware, hacking, child pornography, malware, credit or debit card frauds, disinformation- harming an individual, property or a nation.

Hierarchy of courts, Civil and criminal jurisdictions.

Senior Civil Judge Court, Principal Junior Civil Judge Court and Junior Civil Judge Court are the Subordinate Courts in civil cases. Chief Judicial Magistrate, First Class Judicial Magistrate Court and Second Class Judicial Magistrate Court are the Subordinate Courts in criminal cases.

Jurisdiction of Subordinate Court

The Code of Criminal Procedure provided provisions for the jurisdiction in criminal matters.

Section 14 of the CrPC deals with the local jurisdiction of Judicial Magistrates. This section empowers the Chief Judicial Magistrate, who is subjected to the control of the High Court that he can define the local limits of the areas from time to time, within which the Magistrates exercise all or any of the powers with which they are invested under this code:

1. It is provided that the Special Judicial Magistrate Court may hold its sitting at any place within its local jurisdiction.

2. If the exception is provided by such definition then the powers of the Magistrate and its local jurisdiction shall extend throughout the district.
3. Where the local jurisdiction of a Magistrate has been extended beyond the district of its jurisdiction or the metropolitan area, as the case may be in which he generally holds court, any reference in this code to the Court of Session, Chief Metropolitan Magistrate or the Chief Judicial Magistrate, in relation to such magistrate, throughout the area which comes under his local jurisdiction, be interpreted, unless the circumstances otherwise requires, as a reference to the Court of Session, Chief Judicial Magistrate, or Chief Metropolitan Magistrate, as the case may be exercising jurisdiction in relation to that district or metropolitan area.

Section 22 of the CrPC deals with the local jurisdiction of Executive Magistrates. This section empowered the District Court, which is subjected to the control of the State Government, that it can draw the local limits of the areas under which the Executive Magistrates may use all or any of the powers with which they may be endowed under this code but there are exceptions when the powers and jurisdiction of such Magistrate shall extend throughout the district.

Section 27 of the CrPC deals with the jurisdiction in the case of juveniles. If the accused is under the age of sixteen years then the case is tried by the Court of the Chief Judicial Magistrate or by any court which is tried under the Children Act, 1960.

Section 177 to Section 189 of the CrPC deals with the provisions related to inquiries and trials of the jurisdiction of the Criminal Courts.

Section 177 of the CrPC provides that the court which comes under the local jurisdiction where the offence has been committed then that offence must be inquired and tried by that court.

Section 178 of the CrPC deals with the provisions related to the place where trial or enquiry of offence should be commenced when there is uncertainty regarding the place of commencement of offence.

Section 179 of the CrPC provides that the trial of the offence is commenced at the place of the act where it is done or the place where the consequence ensues.

Section 180 of the CrPC provided the provisions for a place of trial in a situation where an act becomes offence due to another offence.

In case of certain offences, Section 181 of the CrPC provides provisions for the place of trial for such offences.

Section 182 of the CrPC deals with the offences which are committed by telecommunication messages or by letters etc.

Section 183 of the CrPC deals with the offences which are committed during journey or voyage.

Section 184 of the CrPC deals with the offences which are triable together and provide provisions for such offences.

Section 185 of the CrPC empowered the State Government to direct any cases or class of cases can be tried in a Sessions Court for which the trial has been committed in any district.

Section 186 of the CrPC empowered the High Court to decide the district where the trial or inquiry of offence should be commenced in cases where there is confusion regarding the place of trial.

Section 187 of the CrPC empowers the Magistrate to issue warrant or summons for the offence which is committed beyond the local jurisdiction.

Section 188 of the CrPC describes the offences which are committed outside the territory of India.

Section 189 of the CrPC provides the authority to the Central Government that it can take the receipt of evidence for the offences which are committed outside the territory of India.

The Code of Civil Procedure, 1908, provided provisions for the jurisdiction in case of civil matters.

Section 15 of the CPC provides that the suit for the offence firstly have to be instituted in the Court of the lowest grade competent for the trial.

Section 16 of the CPC provided that where suits have to be instituted, should be based on the subject matter which is subject to the pecuniary or other limitations prescribed by the law.

Section 17 of the CPC provided that the suits for the immovable property have to be filed within the local limits of whose jurisdiction where any part of the property is situated.

Section 18 of the CPC provided provisions for the place of institution of the suit where local limits of the jurisdiction of Courts are uncertain.

Section 20 of the CPC provided provisions for the place of institution of other suits. It states that suits for the offence have to be instituted where the cause of action arises or at the place where the defendants reside.

Conclusion

It is evident from this article that the Constitution of India played a crucial role in the rules and laws which are enforced from time to time to strengthen the judicial system of the country. The three-layer judicial system is necessary for the proper functioning of the judiciary in a big country like India to ensure proper justice to the citizens of a country. Every day a lot of disputes were raised, so proper hierarchy of courts and their jurisdiction should be properly defined to deal with such disputes.

Cyberspace-Web space

What Does Cyberspace Mean?

Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

In the common IT lexicon, any system that has a significant user base or even a well-designed interface can be thought to be “cyberspace.”

Techopedia Explains Cyberspace

Cyberspace allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

The term cyberspace was initially introduced by William Gibson in his 1984 book, *Neuromancer*. Gibson criticized the term in later years, calling it “evocative and essentially meaningless.” Nevertheless, the term is still widely used to describe any facility or feature that is linked to the Internet. People use the term to describe all sorts of virtual interfaces that create digital realities.

More on Cyberspace

In many key ways, cyberspace is what human societies make of it.

One way to talk about cyberspace is related to the use of the global Internet for diverse purposes, from commerce to entertainment. Wherever stakeholders set up virtual meeting spaces, we see the cyberspace existing. Wherever the Internet is used, you could say, that creates a cyberspace. The prolific use of both desktop computers and

smartphones to access the Internet means that, in a practical (yet somewhat theoretical) sense, the cyberspace is growing.

Another prime example of cyberspace is the online gaming platforms advertised as massive online player ecosystems. These large communities, playing all together, create their own cyberspace worlds that exist only in the digital realm, and not in the physical world, sometimes nicknamed the “meatspace.”

To really consider what cyberspace means and what it is, consider what happens when thousands of people, who may have gathered together in physical rooms in the past to play a game, do it instead by each looking into a device from remote locations. As gaming operators dress up the interface to make it attractive and appealing, they are, in a sense, bringing interior design to the cyberspace.

In fact, gaming as an example, as well as streaming video, shows what our societies have largely chosen to do with the cyberspace as a whole. According to many IT specialists and experts, including F. Randall Farmer and Chip Morningstar, cyberspace has gained popularity as a medium for social interaction, rather than its technical execution and implementation. This sheds light on how societies have chosen to create cyberspace.

Theoretically, the same human societies could create other kinds of cyberspace—technical realms in which digital objects are created, dimensioned and evaluated in technical ways. For example, cyberspaces where language translation happens automatically in the blink of an eye or cyberspaces involving full-scale visual inputs that can be rendered on a 10-foot wall

In the end, it seems that the cyberspaces that we have created are pretty conformist and one-dimensional, relative to what could exist. In that sense, cyberspace is always evolving, and promises to be more diverse in the years to come.

Web hosting and web Development agreement

In today's time, companies need to have a portfolio on the web or the platform of it's own to offer their service and market themselves. Company hires some other party to complete this project for them i.e, Web Development agencies, And here comes the main process which most of the startups skips finding it of no Use, A website Development contract or a Simple website Development Agreement Document

In this article we are going to discuss the Importance of Agreement between a startup and A web development agency. Also, we have drawn out 5 important reasons, of Why Website Development Agreement India is important.

Agreement for website development between a company and the web developer that assigns the responsibilities, duties, liabilities, terms and conditions of both the parties. The main objective of a web development contract is to ensure that the company gets the website created that it requires by assigning the obligation on the web developer to create the site according to the company's specifications and requirements and which shall be governed by the Indian Contract Act, and with other relevant laws and regulations that may be subject to compliance like IT Act, Copyright Act etc.

Importance to have a Website Development Agreement

- It helps in saving time and is an efficient way of developing websites as professionals are hired to do the task as it provides clarity in understanding the scope of work and deliverables.

- It protects the confidential information of the company by restricting the developers to share the information with third parties.

- A well-defined development contract removes the possibility of misunderstanding, confusion, and disputes between the parties.

- It helps in proper and efficient functioning of the website as per the changing need and demand of the platform

Legal and of domain Names

A domain name is not protected under any law in India. Thus, any person or business obtains protection to a newly created domain name in India under the Trade Marks Act, 1999 and the Trade Marks Rules, 2002. At the international level, the domain names as trademarks are registered by only the ICANN (Internet Corporation for Assigned Names and Numbers) organisation.

At the international level, the domain names as trademarks are protected by the ICANN along with the diverse International Trademark Treaties of the world and the directly concerned national Trademark Law.

After the domain name is registered as a trademark under the Trademarks Act, 1999 (‘Act’), the registered domain name owner will have all rights and authorities that the registered trademark owners avail in India. It will be granted protection as a trademark under the Act’s provisions, including the right to sue for infringement or passing off.

Any person using a domain name registered as a valid and subsisting trademark under the Act in an unauthorised manner will be held liable for infringement of the trademark of the domain name under Section 29 of the Act.

The owners of unregistered trademarks are also entitled to the protection of trademark if they are the prior user of the mark and it has acquired distinctiveness. When there is a misrepresentation of the unregistered mark by anyone else representing them to be his/her goods, and it is likely to deceive the relevant public, the unregistered trademark owner can sue for passing off.

Domain names serve as significant elements in trade and any commercial activity on the internet. Especially the businesses that work solely on the online platform require the protection of their domain names. In India, the Trademarks Act, 1999, confer protection to the domain names in the world. Thus, registered domain names can obtain the protection of trademark infringement, and the unregistered domain name can get the protection of passing off under the Act.

What is a Domain Name?

A domain name is an identification or the interest address of a business. Many top brand business owners use their brand names as domain names. It is not mandatory to purchase the domain name exactly the same as your brand name. But I will recommend purchasing the domain name with your brand name.

Therefore, the best way to remember and recognize your brand name is a perfect and unique domain name. It helps strategize your brand name across marketing channels. Domain Name can be used once after the registration.

However, Domain names can be a combination of alphabets and numbers letters. But I would recommend avoid using numbers in the domain name. Because the number will confuse users to remember and search.

For Example way2digital, it is easy to say but when writing it could be like “waytwodigital” or “way to digital” or “way2digital”

Similarly, there is a possibility to the same domain names with different domain extensions like COM (www.domain.com), or.IN (www.domain.in) and etc. Based on demand and the huge growth of industries, competitors the domain extensions are also been developed.

Significance of Domain Name?

There is much importance of domain names in the digital world of 2020. With the digital transformation of technology, the use of smartphones and the internet, mobile internet data availability and power of social media help the business to grow. Therefore, to empower the growth of business and brand visibility in the internet world the primary thing is a domain name.

“The domain name is nothing but the foundation of your business“.

- It increases your online presence in the digital world or geographic locations.
- The most convenient way to get connected with your audience at their fingertips.
- Adds credibility to small or meddle level business.
- Increases your brand reputation for business
- Increases trust in a walk-in business.

- The best user experience of your product and services.
- Empower your business demand and revenue growth.

How Does Domain Work?

When you enter the domain name or website in your browser or any search engine (like Google, Yahoo, or Bing) instantly sends a request to find that site. The browser opens up with all your product or service information available on your website. Similarly, the search engine result page gives multiple websites or domain name information.

Internet as a tool for global access

Global internet access creates an equal playing field for both the most and least developed countries in our world socially, politically, and economically. Bridging the digital divide requires hard work from the public, private, and nonprofit sectors.

Part of the U.N.'s goals in the 2030 Agenda for Sustainable Development is to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in the least developed countries by 2020."
In 2015, 54 percent of people in developing countries reported using the internet at least occasionally. Eighty-seven percent reported using the internet in developed countries in the same year.

The World Economic Forum described how the internet boosts economies in developing countries through increasing efficiency and productivity in many industries, and also provides financial, health, and educational services to those in developing countries.

Also, social media empowers people to rebel against dictatorships. For example, in 2011, Egyptian citizens organized protests against former President Hosni Mubarak using Facebook and Twitter. Similarly, in 2013, Turkish citizens turned to social media outlets such as Facebook, Twitter, Ustream, and Vine for information on protests, since formal media outlets were censored.

Unit-2

Information Technology Act

Overview of IT Act, 2000

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce. The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- **First Schedule –**
  Deals with documents to which the Act shall not apply.
- **Second Schedule –**
  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.

7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.

Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

Amendments and Limitations of IT Act

Amendments of IT Act: The Information Technology Amendment Act 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act 2000.

The Information Technology Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The act is administered by the Indian Computer Emergency Response Team (CERT-In) and corresponds to the Indian Penal Code.

The Information Technology Amendment Act has been widely hailed as a progressive step forward in protecting India's cyber infrastructure and citizens.

It is one of the most comprehensive pieces of legislation addressing IT-related issues and sets a strong precedent for other countries working to update their own laws.

Why was the Information Technology Amendment Act created?

The original version of the act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime.

However, it also sought to foster security practices within India that would serve the country in a global context.

In addition, the Information Technology Amendment Act established the office of the Cyber Appellate Tribunal to hear appeals from any person aggrieved by an order made under the act.

What does the Information Technology Amendment Act cover?

The Information Technology Amendment Act 2008 has nine chapters and 117 sections and covers a wide range of topics related to IT, cybercrime and data protection.

The act includes provisions for the following

- tightening cybersecurity measures
- establishing a legal framework for digital signatures
- recognizing and regulating intermediaries
- regulating interception, monitoring and decryption of electronic records
- cyber forensics
- cyberterrorism

Amendments to the act have been created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

Digital Signature

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many

engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories −

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use −

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable “OK” or “I Accept” or “I Agree” click boxes

Cryptographic Algorithm

Cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher messages in a cryptographic system. In simple terms, they're processes that protect data by making sure that unwanted people can't access it. These algorithms have a wide variety of uses, including ensuring secure and authenticated financial transactions.

Most **cryptography** algorithms involve the use of **encryption**, which allows two parties to communicate while preventing unauthorized third parties from

understanding those communications. Encryption transforms human readable plaintext into something unreadable, also known as *ciphertext*.
The **encrypted** data is then decrypted to restore it, making it understandable to the intended party. Both **encryption and decryption** operate based on algorithms.

There are many different types of cryptographic algorithms, though most of them fit into one of two classifications — symmetric and asymmetric. Some systems, however, use a hybrid of both classifications. Symmetric algorithms, also known as symmetric-key or shared-key algorithms, work by the use of a key known only to the two authorized parties. While these can be implemented in the form of block ciphers or stream ciphers, the same key is used for both encrypting and decrypting the message. The **Data Encryption** Standard (DES) and **Advanced Encryption Standard** (AES) are the most popular examples of **symmetric cryptography** algorithms.

Asymmetric cryptography algorithms rely on a pair of keys — a public key and a private key. The public key can be revealed, but, to protect the data, the private key must be concealed. Additionally, encryption and decryption of the data must be done by the associated private and public keys. For example, data encrypted by the private key must be decrypted by the public key, and vice versa. RSA is one of the most common examples of this **algorithm**.

Symmetric algorithms are usually much faster than asymmetric algorithms. This is largely related to the fact that only one key is required. The disadvantage of shared-key systems, however, is that both parties know the secret key. Additionally, since the algorithm used is the public domain, it is actually the

key that controls access to the data. For these reasons, the keys must be safe-guarded and changed relatively frequently to ensure security.

Public Cryptography

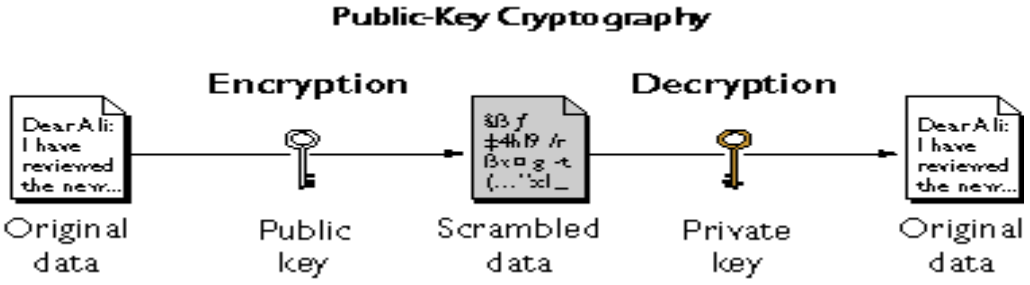
The most commonly used implementations of public key cryptography (also known as public-key encryption and asymmetric encryption) are based on algorithms presented by Rivest-Shamir-Adelman (RSA) Data Security.

Public key cryptography involves a pair of keys known as a public key and a private key (a *public key pair*), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key.

RSA public key pairs can be any size. Typical sizes today are 1024 and 2048 bits.

Public key cryptography enables the following:

- Encryption and decryption, which allow two communicating parties to disguise data that they send to each other. The sender encrypts, or scrambles, the data before sending it. The receiver decrypts, or unscrambles, the data after receiving it. While in transit, the encrypted data is not understood by an intruder.
- Nonrepudiation, which prevents:
    - The sender of the data from claiming, at a later date



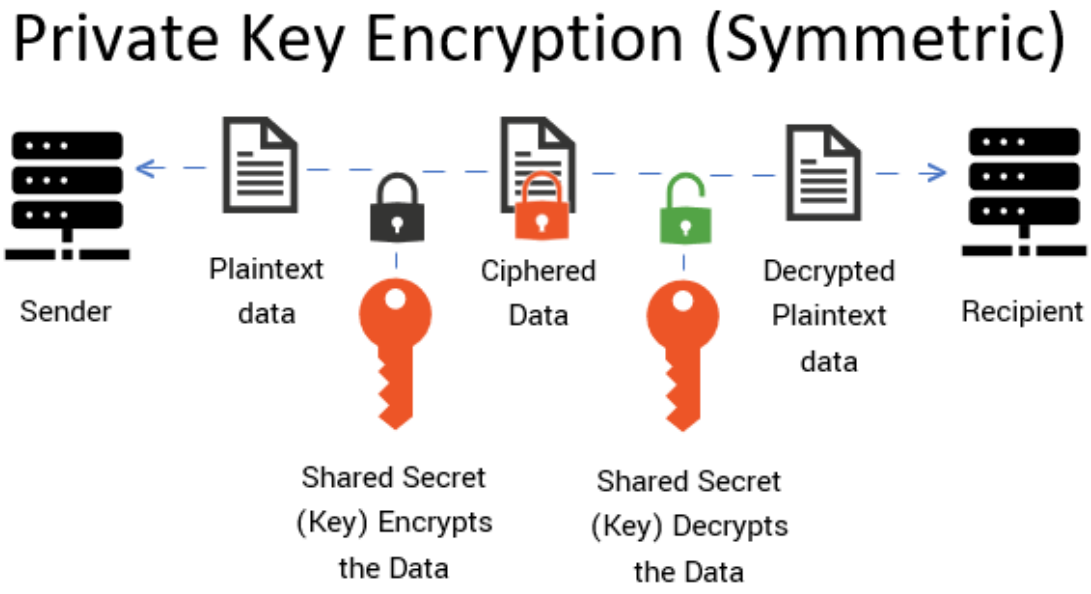
shows how you can freely distribute the public key so that only you (the owner of the private key) can read data that was encrypted with the public key. In general, to send encrypted data to someone, you must encrypt the data with that person's public key, and the person receiving the data decrypts it with the corresponding private key.

If you compare symmetric-key encryption with public-key encryption, you will find that public-key encryption requires more calculations. Therefore, public-key encryption is not always appropriate for large amounts of data. However, it is possible to use public-key encryption to send a symmetric key, which you can then use to encrypt additional data.

Private Cryptography

Private key encryption is the original type of encryption. Dating back to the advent of cryptography, private key cryptosystems were the first and continue to be the most common. When using private key cryptography, both parties much each possess, or at least exchange the private key. The word “key” can be a bit misleading — the key itself is really just the cipher that’s used to scramble and unscramble the data being encrypted.
With an ancient cipher, like the Caesar cipher, the private key was simply a number that corresponded to the number each alphabetical character needed to be shifted. In current digital encryption schemes, the keys are now prohibitively difficult algorithms that no modern computer could ever efficiently crack.

The one thing that remains the same with all private key systems is that the same key can both encrypt and decrypt. Private key encryption is sometimes called symmetric encryption.



What is Private Key Cryptography Used for?

Public key cryptography, in the context of SSL/TLS, is used for the actual communication portion of the connection. Each party derives the key during the handshake and then uses it to both encrypt and decrypt all data that's transmitted between them.

Private key encryption, or symmetric encryption, uses smaller keys that are easier to compute with. These still provide adequate computational hardness, but don't tax the client and server as much to use. Especially at scale, this is extremely important and the biggest advantage of symmetric encryption.

Electronic Governance

Electronic governance or e-governance is adopted by countries across the world. In a fast-growing and demanding economy like India, e-governance has become essential. The rapid growth of digitalisation has led to many governments across the globe to introduce and incorporate technology into governmental processes. Electronic

governance or e-governance can be defined as the usage of Information and Communication Technology (ICT) by the government to provide and facilitate government services, exchange of information, communication transactions and integration of various standalone systems and services.

In other words, it is the use of technology to perform government activities and achieve the objectives of governance. Through e-governance, government services are made available to citizens and businesses in a convenient, efficient and transparent manner. Examples of e-governance include Digital India initiative, National Portal of India, Prime Minister of India portal, Aadhaar, filing and payment of taxes online, digital land management systems, Common Entrance Test etc.

Types of interactions in e-Governance

e-Governance can take place in four major types of interactions, apart from the processes and interactions in the back-office, within the government framework:

Government to Government (G2G)

Information is exchanged within the government i.e., either, between the central government, state government and local governments or between different branches of the same government.

Government to Citizen (G2C)

The citizens have a platform through which they can interact with the government and get access to the variety of public services offered by the Government.

Government to Businesses (G2B)

The businesses are able to interact with the government seamlessly with respect to the services of the government offered to businesses

Government to Employees (G2E)

The interaction between the government and its employees occurs in an efficient and speedy manner.

Objectives of e-Governance

The objectives of e-governance can be listed down as given below:

- To support and simplify governance for government, citizens, and businesses.
- To make government administration more transparent and accountable while addressing the society's needs and expectations through efficient public services and effective interaction between the people, businesses, and government.
- To reduce corruption in the government.

- To ensure speedy administration of services and information.
- To reduce difficulties for business, provide immediate information and enable digital communication by e-business.

While e-governance provides the advantages of convenience, efficiency and transparency, it also has problems associated with it. They are as follows:

- Lack of computer literacy: India is still a developing country and a vast majority of the citizens lack computer literacy which hinders the effectiveness of e-governance.
- Lack of accessibility to the internet or even computers in some parts of the country is a disadvantage to e-governance.
- e-Governance results in a loss of human interaction. As the system becomes more mechanised, lesser interaction takes place among people.
- It gives rise to the risk of personal data theft and leakage.
- e-Governance leads to a lax administration. The service provider can easily provide excuses for not providing the service on technical grounds such as “server is down” or “internet is not working”, etc.

e-Governance in the Indian context

e-Governance in India is a recently developed concept. The launch of National Satellite-Based Computer Network (NICENET) in 1987 and subsequent launch of the District Information System of the National Informatics Centre (DISNIC) programme to computerise all district offices in the country for which free hardware and software was offered to the State Governments provided the requisite impetus for e-governance.

e-Governance thereafter developed with the growth of technology. Today, there are a large number of e-Governance initiatives, both at the Union and State levels. In 2006, the **National e-Governance Plan** (NeGP) was formulated by the Department of Electronics and Information Technology and Department of Administrative Reforms and Public Grievances that aims at making all government services accessible to the common man, ensure efficiency, transparency and reliability of such services at affordable costs to realise the basic needs of the common man.

The NeGP has enabled many e-governance initiatives like:

- **Digital India** was launched in 2015 to empower the country digitally. Its main components are:
  - Developing a secure and stable digital infrastructure
  - Delivering government services digitally
  - Achieving universal digital literacy

- **Aadhaar** is a unique identification number issued by UIDAI that serves as proof of identity and address on the basis of biometric data. It is being used to provide many benefits to the members of the society. One can **e-sign** documents using Aadhar.
- **myGov.in** is a national citizen engagement platform where people can share ideas and be involved with matters of policy and governance.
- **UMANG** is a Unified Mobile Application which provides access to central and state government services including Aadhar, Digital Locker, PAN, Employee Provident Fund services, etc.
- **Digital Locker** helps citizens digitally store important documents like mark sheets, PAN, Aadhar, and degree certificates. This reduces the need for physical documents and facilitates easy sharing of documents.
- **PayGov** facilitates online payments to all public and private banks.
- **Mobile Seva** aims at providing government services through mobile phones and tablets. The m-App store has over 200 live applications which can be used to access various government services.
- **Computerisation of Land Records** ensures that landowners get digital and updated copies of documents relating to their property.

In addition to the above, State level e-governance initiatives include:

- **E-Seva** (Andhra Pradesh) facilitates payment of utility bills, issuance of certificates, licenses and permits.
- **Khajane Project** (Karnataka) digitalized the treasury system of the state.
- **FRIENDS** (Kerala) is a single-window facility to pay taxes and other financial dues to the State government.
- **Lokvani Project** (Uttar Pradesh) is a single-window solution relating to the handling of grievances, land record maintenance and providing a mixture of essential services.

e-Governance Portal of India

The Indian e-governance portal is https://nceg.gov.in. On this portal, one can get comprehensive information regarding the National Conference on e-Governance and reports on earlier conferences.

Additionally, the portal provides links to the following important pages:

- Digital India
- National Portal of India: It is developed to provide access to information and services being provided by the government
- PM India Website: provides information relating to the Prime Minister's Office.
- United Nations e-governance website

Legal Recognition of Electronic Records

According to the World Bank, E-Governance is when government agencies use information and communication technologies to transform relations with citizens, businesses, and other government agencies. One of the prime objectives of the IT Act, 2000 is the promotion of electronic governance. In this article, we will talk about electronic records and e-governance.

In the IT Act, 2000, there are special provisions under Chapter III to grant legal recognition to electronic records, signature, and also encourage the government and its agencies to use them.

Provisions for e-governance under the IT Act, 2000

These are the provisions under the IT Act, 2000 in the context of e-governance:

1. Legal Recognition of Electronic Records (Section 4)

Let's say that a certain law requires a matter written, typewritten, or printed. Even in the case of such a law, the requirement is satisfied if the information is rendered or made available in an electronic form and also accessible for subsequent reference.

2. Legal recognition of digital signatures (Section 5)

Let's say that the law requires a person's signature to authenticate some information or a document. Notwithstanding anything contained in such law, if the person authenticates it with a digital signature in a manner that the Central Government prescribes, then he satisfies the requirement of the law.

For the purpose of understanding this, signature means a person affixing his handwritten signature or a similar mark on the document.

3. Use of electronic records and digital signatures in Government and its agencies (Section 6)

(1) If any law provides for –

a. the filing of a form, application, or any document with any Government-owned or controlled office, agency, body, or authority

b. the grant or issue of any license, sanction, permit or approval in a particular manner

c. also, the receipt or payment of money in a certain way

Then, notwithstanding anything contained in any other law in force such as filing, grant, issue, payment, or receipt is satisfied even if the person does it in an electronic form. The person needs to ensure that he follows the Government-approved format.

(2) With respect to the sub-section (1), may prescribe:

a. the format and manner of filing, creating or issuing such electronic records

b. also, the manner and method of payment of any fees or charges for filing, creating or issuing any such records

4. Retention of electronic records (Section 7)

(1) Let's say that the law requires the retention of certain records, documents or information for a specific period. In such cases, the requirement is also satisfied if the retention is in an electronic form, provided:

a. the information contained therein is accessible and also usable for a subsequent reference.
b. the format of the electronic record is the same as the one originally created, received or sent. Even if the format is changed, then it must accurately represent the original information.
c. the electronic record contains details to facilitate the identification of the origin, destination, and also the date and time of the dispatch or receipt of the record.

This is provided that the clause does not apply to any information which is automatically generated primarily for the purpose of enabling an electronic record for dispatch or receipt.

(2) Nothing in this section applies to any law which expressly provides for the retention of records, documents or information electronically.

5. Publication of rules, regulations, etc., in Electronic Gazette (Section 8)

Let's say that law requires the publishing of official regulation, rule, by-law, notification or any other matter in the Official Gazette. In such cases, the requirement is also satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette.

However, the date of publication of the rule, regulation, by-law, notification or any other matter is the date of the Gazette first published in any form – Official or Electronic.

6. Section 6,7 and 8 do not confer a right to insist document should be accepted in Electronic form (Section 9)

It is important to note that, nothing contained in Sections 6, 7, and 8 confer a right upon any person to insist either the acceptance, issuance, creation or also retention of any document or a monetary transaction in the electronic form from:

- Ministry or Department of the Central/State Government
- Also, any authority or body established under any law by the State/Central Government

7. Power to make rules by Central Government in respect of digital signature (Section 10)

The IT Act, 2000 empowers the Central Government to prescribe:

- Type of digital signature
- Also, the manner and format of affixing the digital signature
- Procedures which facilitate the identification of the person affixing the digital signature
- Control processes and procedures to ensure the integrity, security, and confidentiality of electronic payments or records
- Further, any other matter which is legally important for digital signatures

Certifying Authorities

A certificate signed by a Certificate Authority (CA) that is trusted by the browser is visually displayed as trusted, usually by showing a padlock. A browser trusts the CA if the CA's public root certificate is installed in the browser and/or computer you are using. Browsers

come with a set of pre-installed CA certificates and only trust sites signed by any of the pre-installed CA certificates. We will refer to the browser's pre-installed CA certificates as "well known Certificate Authorities". Examples include Comodo, GeoTrust, and Symantec.

Benefits in being your own CA and using our free CA tool

Becoming a Certificate Authority (CA) simply means that you (or your customers) are in charge of the issuing process of cryptographic pairs of private keys and public certificates. With that said, anyone can literally become their own Certificate Authority and there are no implied restrictions or authorizations necessary.

There are no costs associated with being your own CA or for your customers to be their own CA.

You can find several tutorials on the internet that explain how to use the OpenSSL command line tool for setting up your own CA infrastructure. If you are new to X.509 certificate chain of trust, these tutorials will make your head spin. In addition, the OpenSSL command line tool is a bit cumbersome to use and gives difficult to understand error messages if you make mistakes.

To make it much easier to be your own CA, we created this free tool that wraps around OpenSSL and provides a graphical user interface to this command line tool. The application includes a wizard that makes it very easy to create a root CA and to create any number of certificates signed by the root CA. In other words, the application makes it very easy to create your own chain of trust. The application is self-contained, and you simply download the tool and run it on your computer.

Cyber Crime and Offences

cybercrime, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through

the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

Defining cybercrime

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

Network Service Providers Liability

The Internet serves as a powerful mechanism for the collaboration, communication and interaction between individuals regardless of their geographic location. It has proven to be a tremendous success - connecting more than 100 million computers and is further growing beyond the wildest expectations of the *Homo sapiens*.

Internet users cannot be regarded as a homogenous group. It is imperative to distinguish the liability of those who give individuals and corporations access to the Internet from that of individual users. The former includes not only Internet Service Providers (ISPs) but also non-commercial hosts such as universities, offices, other educational institutions, corporate sectors etc.

ISP is an entity that connects people to the Internet and provides related services such as web site building and hosting. ISPs are also sometimes described as Online Service Providers. ISPs are today largely immune from liability for their role in the creation and propagation of worms, viruses, obscene and defamatory material and other forms of malicious computer codes. In the spirit of promoting electronic transactions, it becomes all the more essential to clarify the position regarding the liability of the ISPs. Amidst this scenario, this paper makes a sincere attempt to analyse the concepts of Cyberspace, Network, Internet and ISP.

Cyber Regulations Appellate Tribunal

The composition of Cyber Appellant Tribunal (Section 49)

The Central Government appoints only one person in a Tribunal – the Presiding Officer of the Cyber Appellate Tribunal.

The qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal (Section 50)

A person is considered qualified for the appointment as the Presiding Officer of a Tribunal if –

a. He has the qualification of the Judge of a High Court
b. He is or was the member of the Indian Legal Service and holds or has held a post in Grade I of that service for at least three years.

The Term of Office (Section 51)

The Term of Office of the Presiding Officer of a Cyber Appellate Tribunal is five years from the date of entering the office or until he attains the age of 65 years, whichever is earlier.

Filling up of vacancies (Section 53)

If for any reason other than temporary absence, there is a vacancy in the Tribunal, then the Central Government hires another person in accordance with the Act to fill the vacancy. Further, the proceedings continue before the Tribunal from the stage at which the vacancy is filled.

Resignation and removal (Section 54)

1. The Presiding Officer can resign from his office after submitting a notice in writing to the Central Government, provided:
    a. he holds office until the expiry of three months from the date the Central Government receives such notice (unless the Government permits him to relinquish his office sooner), OR
    b. he holds office till the appointment of a successor, OR
    c. until the expiry of his office; whichever is earlier.
2. In case of proven misbehaviour or incapacity, the Central Government can pass an order to remove the Presiding Officer of the Cyber Appellate Tribunal. However, this is only after the Judge of the Supreme Court conducts an inquiry where the Presiding Officer is aware of the charges against him and has a reasonable opportunity to defend himself.
3. The Central Government can regulate the procedure for the investigation of misbehaviour or incapacity of the Presiding Officer.

Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings (Section 55)

According to this section, no order of the Central Government appointing any person as the Presiding Officer of the Tribunal can be questioned in any manner. Further, no one can question any proceeding before a Cyber Appellate Tribunal in any manner merely on the grounds of any defect in the Constitution of the Tribunal.

Appeal to Cyber Appellate Tribunal (Section 57)

1. Subject to the provisions of sub-section (2), a person not satisfied with the Controller or Adjudicating Officer's order can appeal to the Cyber Appellate Tribunal having jurisdiction in the matter.

2. No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
3. The person filing the appeal must do so within 25 days from the date of receipt of the order from the Controller or Adjudicating Officer. Further, he must accompany the appeal with the prescribed fees. However, if the Tribunal is satisfied with the reasons behind the delay of filing the appeal, then it may entertain it even after the expiry of 25 days.
4. On receiving an appeal under sub-section (1), the Tribunal gives an opportunity to all the parties to the appeal to state their points, before passing the order.
5. The Cyber Appellate Tribunal sends a copy of every order made to all the parties to the appeal and the concerned Controller or adjudicating officer.
6. The Tribunal tries to expeditiously deal with the appeals received under sub-section (1). It also tries to dispose of the appeal finally within six months of receiving it.

Penalties and Adjudication.

(1) The Central Government may, by an order published in the Official Gazette, appoint an officer of the Central Government, not below the rank of Joint Secretary to the Government of India or equivalent, as adjudicating officer for adjudging penalties under the provisions of this Act.

(2) The adjudicating officer may, on a complaint made in writing by a person authorised by the Corporation, and after giving a reasonable opportunity of being heard, by an order impose penalty on a director or employee liable to penalty under any provision of this Act on account of any contravention or violation on his part.

(3) The adjudicating officer, for the purposes of discharging his functions under this Act, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a suit, to summon and enforce the attendance of any person and examine him on oath and to require the discovery and production of documents or other electronic records, and shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.

(4) A director or employee aggrieved by any order made by the adjudicating officer may prefer an appeal to such officer to the Central Government of a rank higher than that of the adjudicating officer as the Central Government may appoint as appellate authority, within thirty days from the date on which a copy of the order made by the adjudicating officer is received by the aggrieved individual, and the officer so appointed may, after giving the individual an opportunity of being heard, pass such order as he may deem fit, confirming, modifying or setting aside the order appealed against, or remanding the case to the adjudicating officer for disposal, with such directions as he may deem fit.

(5) Where a director or employee of the Corporation having already been subjected to penalty under this Act for any contravention or violation of any provision of this Act, again commits such contravention or violation within a period of three years from the date of order imposing such penalty passed by the adjudicating officer, he shall be liable for the second or subsequent contravention or violation for twice the amount of penalty provided therefor.

Unit-3:

Cyber Law and Related Legislation

What Is a Patent?

A patent safeguards an original invention for a certain period of time and is granted by the United States Patent and Trademark Office (USPTO). By granting the right to produce a product without fear of competition for the duration of the patent, an incentive is provided for companies or individuals to continue developing innovative new products or services.1

There are three types of patents: utility patents, plant patents, and design patents.

1. **Utility Patent**

A Utility Patent covers the creation of a new or improved product, process, or machine. Also known as a “patent for invention,” it bars other individuals or companies from making, using, or selling the creation without consent. Utility patents are good for up to 20 years after the patent application is filed, but require the holder to pay regularly scheduled maintenance fees.3

While most people associate patents with machines and appliances, they can also apply to software, business processes, and chemical formulations such as in pharmaceutical products.

2. **Plant Patent**

A plant patent protects a new and unique plant’s key characteristics from being copied, sold, or used by others. It is also good for 20 years after the application is filed. The plant must be asexually reproducible with reproduction being genetically identical to the original and performed through methods such as root cuttings, bulbs, division, or grafting and budding.

3. **Design Patent**

A Design patent on the other hand, applies to the unique look of a manufactured item. Take, for example, an automobile with a distinctive hood or headlight shape. These visual elements are part of the car’s identity and may add to its value; however, without protecting these

components with a patent, competitors could potentially copy them without legal consequences.

The total number of patents issued in the United States in 2021.
Design patents issued since May 2015 last for 15 years from the date the patent is granted and do not require maintenance fees. Patents issued prior to that last for 14 years.

What Is a Trademark?

Unlike patents, a trademark protects words and design elements that identify the source of a product. Brand names and corporate logos are primary examples. A service mark is similar, except that it safeguards the provider of a service instead of a tangible good. The term “trademark” is often used in reference to both designations.

Some examples of trademark infringement are fairly straightforward. You’ll probably run into trouble if you try to bottle a beverage and call it Coca-Cola or even use the famous wave from its logo since both have been protected for decades.

However, a trademark actually goes a bit further, prohibiting any marks that have a “likelihood of confusion” with an existing one. Therefore, a business can’t use a symbol or brand name if it looks similar, sounds similar, or has a similar meaning to one that’s already on the books, at least if the products or services are related. If the trademark holder believes there’s a violation of these rights, it may decide to sue.

What Is a Copyright?

Copyright protect “original works of authorship,” such as writings, art, architecture, and music. For as long as the copyright is in effect, the copyright owner has the sole right to display, share, perform, or license the material.

One notable exception is the “fair use” doctrine, which allows some degree of distribution of copyrighted material for scholarly, educational, or news-reporting purposes.

Technically, you don’t have to file for a copyright to have the piece of work protected. It’s considered yours once your ideas are translated into a tangible form, such as a book, music, or published research; however, officially registering with the U.S. Copyright Office before—or within five years of—publishing your work makes it a lot easier to establish that you were the original author if you ever have to go to court.

The duration of a copyright depends on the year it was created, as the laws have changed over the years. Since 1978, most compositions have been copyright-protected for 70 years after the author’s death. After that time, individual works enter the public domain and can be reproduced by anyone without permission.

As a general rule, the author retains ownership of copyright privileges, even if the material is published by another company. There is an important exception to this rule, though.

Materials you create for your employer as part of your job requirements, for example, contributions to a podcast the company publishes, are usually considered "works for hire." The employer, not you, retains the copyright. If there’s a gray area, you can try to negotiate with the publisher over copyright ownership prior to creating the piece; just be sure to get it in writing.

What Is the Difference Between a Patent, Copyright, and Trademark?

A patent protects new inventions, processes, or scientific creations, a trademark protects brands, logos, and slogans, and a copyright protects original works of authorship.

What Are the 3 Types of Patents?

The three types of patents are design, utility, and plant. Utility patents are for new discoveries, compositions of matter, machines, or processes. Plant patents are for anyone that discovers or develops and asexually reproduces a new variety of plant. A design patent is for anyone that creates a new, original, and ornamental design.

The Bottom Line

The decision to pursue a patent, trademark, or copyright depends on the type of intellectual property you’re trying to shield. Whether it’s a new product, logo, or creative work, registering your idea with the appropriate body can help ensure you enjoy the fruits of your labor.

Electronic Data Base and its Protection

An electronic database is a searchable electronic collection of resources. There are two basic types of databases:

- Indexes or bibliographic databases
- Full-text databases.

Indexes or bibliographic databases, also known as indexing and abstracting services, provide:

- Indexing information for topical searching across resources in multiple formats (including multidisciplinary searches)
- Abstracts (short descriptions) of the contents (eg. articles), to help you decide if it is relevant to your research.

Full-text databases provide the same services as above, but also include the full text of articles, allowing you to read it online, or download it for offline reading.

These databases allow the University Library to provide students and staff of Notre Dame with access to thousands of journals, as well as ebooks, newspaper articles, reports; pictures, and streaming video content.

IT Act

An Act 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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United

.Nations Commission on International Trade Law; AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information; AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

Civil procedure code

The code of civil procedure 1908 governs the procedure of the Courts of Civil Judicature. A Code, as defined under Section 2(1) of the Code of Civil Procedure, 1908, is generally a set of rules that regulates the locomotion of a case in a court. The Code of Civil Procedure, 1908 being a procedural law by nature administers civil proceedings in the Indian territory and therefore is recognized as a Code. The Code is made up of 158 sections comprising the substantive part of the Code, and 51 orders comprehending the procedural aspect of the Code. Although there are 51 orders in the Code, this article will specifically focus on the first 21 orders that lays down the basic civil procedure to be followed by a civil court in a case hearing.

- Order: Defined under Section 2(14) of the Code of 1908, the order simply provides as to how a case will move forward in a civil court. As the provision provides, order connotes the formal expression of a Civil Court's decision, but expressly excludes a decree.
- Decree: Defined under Section 2(2) of the Civil Procedure Code, 1908, the decree is also a formal expression of an adjudication that lays down the rights of the parties in a civil case that are the plaintiff, and the defendant. A decree must have the following essential; the rights of the parties, the suit,

adjudication, conclusive determination of the decided rights of the parties, and should be in writing.

- Judgment: Defined under Section 2(9) of the Code of 1908, a judgment is a statement delivered by the Judge in a civil case on the basis of the order, or the decree previously passed by him, or her, to the parties involved in the case. A judgment must consist of the statement of facts, the determining points, the decision of the court, and the reason behind the court's decision.

Order 1 to 21 of the Code of Civil Procedure, 1908

As the Code of Civil Procedure, 1908 is a very significant, and relevant civil procedural law, knowledge about the Orders stands indispensable. Along with that for preparation of any legal competitive examinations, this statute cannot be ignored. Remembering the orders often becomes difficult and therefore, along with the legal explanation, a simple interpretation has also been provided hereunder to make the civil procedure easy to be understood by individuals of both legal, and non-legal background.

Order 1: Parties to Suit

There are always two parties involved in a case. For a civil case, these two parties are referred to as the plaintiff, who is responsible for instituting the suit against the other party, and the defendant who is the other party and has to provide his defense in the civil court against the allegations made on him. This is the beginning of a civil case as have been provided under Order 1 that deals with Parties to suit. Right after the parties to suit are recognized comes the need to frame the suit as provided under Order 2.

Order 2: Frame of Suit

The plaintiff will be approaching a civil court with his suit which is familiarly known as Frame of Suits provided under Order 2 of the Code. Framing of suit signifies that a party has instituted a legal action against another party. As provided by Rule 2 of Order 2, the plaintiff is supposed to include his entire claim in the suit, which will function as a cause of action brought by the plaintiff against the defendant. The framed suit needs to be instituted before the civil court. But, who does the institution? Is it the plaintiff, or any other individual? This question is answered by Order 3 of the Code.

Order 3: Recognized agents and pleaders

Order 3 of the Code of 1908 talks about recognized agents and pleaders. For instituting the suit framed by the plaintiff before the civil court, the instituting party needs the help of a legal professional or a pleader who is expertise in the field of law. Here comes the need to hire a lawyer who takes the framed suit before the civil court on behalf of the aggrieved party, that is the plaintiff. Who all can be categorized as recognized agents, and pleaders have been given room under Rule 2, and Rule 4 of Order 3 respectively. Now it becomes the responsibility of the recognized agent, or a pleader, to institute the suit before the civil court on behalf of the disputed party, the plaintiff, which brings us to Order 4 of the Code.

Order 4: Institution of suits

For instituting the suit, a plaint needs to be presented before the court by the plaintiff. The meaning of a plaint has been explained under Order 7 of the Code of Civil Procedure, 1908. It is to be noted that for the proper institution of suit compliance with sub-rules (1), and (2) of Rule 1 of Order 4 stands mandatory. While sub-rule (1) mandates the presentation of a plaint to institute a suit before the court of law, sub-rule (2) provides that no plaint as provided in the previous rule can escape the rules provided under Order 6, and 7 of the Code.

IT Act and Criminal Procedural Code

The **Code of Criminal Procedure** commonly called **Criminal Procedure Code** (**CrPC**) is the main legislation on procedure for administration of substantive criminal law in India. It was enacted in 1973 and came into force on 1 April 1974. It provides the machinery for the investigation of crime, apprehension of suspected criminals, collection of evidence, determination of guilt or innocence of the accused person and the determination of punishment of the guilty. It also deals with public nuisance, prevention of offences and maintenance of wife, child and parents.

Application of the Criminal Procedure Code

The criminal procedure code (CrPC) applies to India and administers criminal law in India.

It's a machinery for defining procedures for determining the guilt or innocence of a person and collecting evidence.

It also defines jurisdiction in certain offences like offences committed by juveniles and also deals with public nuisance, maintenance of wife, children and parents.

It also describes the powers and jurisdiction of the courts and the offences triable by them.

Objectives of Criminal procedure code (CrPC)

The code of criminal procedure laid down some objectives. These are:-

1. The main aim of this code is to provide an opportunity for a fair trial to the accused person according to the principle of natural justice.

2. To ensure a fair trial for both the accused and the victim without curtailing anyone's rights.
3. To achieve a fair adjudication process by laying criteria for admissibility of evidence.
4. To prevent delaying the investigation and trial process.
5. To ensure attendance of any person concerned with a case with the various available measures like warrant, summons, attachment of property, proclamation, etc.
6. To lay down the criminal justice system's functioning procedure from the stage of investigation till conviction and the process for appeal.
7. To explain the organisation of criminal courts in India.
8. To explain the role and powers of police and other authorities in the investigation and trial process.
9. To explain the powers and jurisdiction of courts in the criminal judicial system.

Features of CrPC (Criminal Procedure Code)

There are some salient features of the criminal procedure code. These are:-

- *Fair trial:* Every person is entitled to a fair trial process, and every person is entitled to a hearing by an independent and impartial court of law.
  No one should judge his cause or in the matter in which he got an interest, and it gets based on the *'Nemo judex in causa sua'* principle, which is the rule against bias.

An accused is presumed innocent until he is proven guilty.
All the accused has the right to be represented by the counsel of his choice.
All the accused are entitled to a fair hearing process, and the ex-parte order should not get passed without hearing them. It gets based on the principle of *'Audi alteram partem'*.

- *Judicial Magistrates are under the purview of High Courts:* All the Judicial Magistrates are under the purview of the High Courts of the concerned states. The Judicial Magistrates posted in Metropolitan cities are known as Metropolitan Magistrates.
  The governor appoints a first-class judicial magistrate in consultation with the public service commission and the high courts.

  The high courts are empowered to appoint a first-class judicial magistrate as a chief judicial magistrate in every district of a respective state.

  The high courts also can appoint additional chief metropolitan magistrates or metropolitan magistrates for a metropolitan court.
- *The organisation of the Criminal Courts in India:* The Criminal Procedure Code (CrPC) provides for setting up a uniform set of criminal courts throughout the territory of India by conferring jurisdiction, powers and functions on them for its smooth functioning.
  It mandates the separation of judiciary from the influence of legislature and executive, which helps the judicial machinery

work independently and impartially without interfering with any other organs of the State.

- *Provisions for the aid of the accused person*- Any accused person can avail of the free legal aid services if the accused person is not in a state to afford litigation financially.
  In petty cases, the accused can plead guilty and deposit the fine by post specified in the summons without appearing in person before the court.

  An accused person has the right to get medically examined to aid him further in the case in his defence.
- *Trial Procedure*- The Procedure for trial will be the same as in both summary cases and summons cases except otherwise. The Sessions court has the power to exercise the revisional jurisdiction and the High Courts.

  Offences punishable with death, life imprisonment and imprisonment exceeding two years will be considered as warrant cases while,

  Offences punishable with fewer than two years imprisonment will get considered as summons cases. The court of law is also empowered to punish a person on the spot found guilty of perjury.
- *Duty of the Police*- A police officer must register an FIR upon receiving a complaint about a request. If he refuses to record FIR about the commission of the crime, the aggrieved person has a right to complain about it to the superintendent of the police.

Need of code of criminal procedure

The Criminal Procedure Code (CrPC) is the machinery to address the need of the criminal justice system and ensure an effortless judicial process by defining the functions of executive and judiciary, respectively.

The code of criminal procedure 1973 is the machinery which fulfilled the needs for:-

1. Registration of a complaint and then an FIR
2. Conducting Investigation of crime
3. Apprehensions of suspected criminals
4. Gathering of evidence
5. Determining the guilt of the accused
6. Determining the innocence of the accused person
7. Determining punishment for the guilty person.

Organisations of Criminal Courts

Hierarchy in the Judicial system gets represented by the first and second class judicial magistrates, chief judicial magistrates, additional district judges and district judges.

All the magistrates deal with the issues of maintaining law and order and preventing crime. All the judicial magistrates function by being under the control of the high court.

The Criminal Procedure Code (CrPC) ensures the independence of the Judiciary from the legislature and executive. The judiciary is not under the control of any of the organs of the state.

The CrPC provides for a uniform set of courts in our criminal justice system throughout the territory of India by defining their jurisdictions, powers and functions.

The Supreme court and High courts are the constitutional courts of India with Jurisdiction, powers and functions.

The High Court can oversee the functioning of all the subordinate courts and tribunals in the concerned state.

Differences Between CrPC and IPC

The significant difference between CrPC and IPC is that IPC lays down the provisions for all the offences and punishments for committing those offences. In contrast, CrPC lays down the procedure followed in the investigation, trial and conviction of that offence.

IPC is substantive law, while CrPC is procedural law.

IPC aims to provide a penal code for punishment to the offenders, while CrPC seeks to make the penal code and other criminal laws more effective.

The Criminal Procedure Code (CrPC)provides for powers of courts and magistrates while IPC is silent on it.

CrPC lays down the procedure for framing of charge while IPC lays down the charges for the respective offences.

Relevant Sections of Indian Evidence Act

The Indian Evidence Act, 1872

THE INDIAN EVIDENCE ACT, 1872

1.Short title, extent and commencement : This Act may be called the Indian Evidence Act, 1872. It extends to the whole of India 1[except the State of Jammu and Kashmir] and applies to all judicial proceedings in or before any Court, including Courts-martial, 2[other than Courts-martial convened under the Army Act] (44 & 45 Vict., c. 58) 3[the Naval Discipline Act (29 & 30 Vict., c. 109) or 4[***] the Indian Navy (Discipline) Act, 1934 (34 of 1934)5 6[or the Air Force Act] (7 Geo. 5, c. 51) but not to affidavits 7presented to any Court or Officer, nor to proceedings before an arbitrator; and it shall come into force on the first day of September, 1872.

2.Repeal of enactments : [Rep. by the Repealing Act, 1938 (1 of 1938), sec. 2 and Sch.]

3 Interpretation clause. —In this Act the following words and expressions are used in the following senses, unless a contrary intention appears from the context:— "Court". —"Court" includes all Judges [1] and Magistrates, [2] and all persons, except arbitrators, legally authorized to take evidence. "Fact". —"Fact" means and includes—

1.any thing, state of things, or relation of things, capable of being perceived by the senses;

2. any mental condition of which any person is conscious.

Illustrations

a. That there are certain objects arranged in a certain order in a certain place, is a fact.

b. That a man heard or saw something, is a fact.

c. That a man said certain words, is a fact.

d.That a man holds a certain opinion, has a certain intention, acts in good faith, or fraudulently, or uses a particular word in a particular sense, or is or was at a specified time conscious of a particular sensation, is a fact.

Relevant Sections of Bankers Book Evidence Act

Introduction

- The Banker’s Book Evidence Act came into effect from 1891.
- When a judge may order a party to inspect and take copies of entries in banker’s books.
- The judge may also order the bank to produce certified copies of the entries accompanied by a further certificate that no other entries in the books of the bank are relevant to the matter of such proceedings.
- Such order shall be served on the bank three clear days exclusive of bank holidays before the same is to be obeyed unless otherwise directed by the court.

Entities Under This Act

- Companies which are defined under the Company act 1956
- Corporate which includes The Reserve Bank Of India, State Bank Of India and its subsidiaries act 1959
- Any company or corporation carrying on the business of banking
- Any partnership or individual to whose books the provision of act can be inferred
- Any Post Office Savings Bank or a money order office

Banker's Book

Banker’s book includes ledgers, day-books, cash-books, account-books and all other records used in the ordinary business of the bank, whether these records are kept in written form or stored in a micro film, magnetic tape or in any other form of mechanical electrical data retrieval mechanism, either onsite or offsite location including a backup.

Certified Copy

- They are maintained in written form a copy of any entry in such books together with a certificate written at the foot of such copy that is true of knowledge. Such entry books are still in custody of the bank further that each should be certified dated and subscribed by the principal accountant or manager with his name and official title
- Contained printout of data stored in a floppy, disc, tape or any other electromagnetic data storage device, a printout together with above statements.
- A printout of an entry from magnetic tape, micro film or in any other form of mechanical or electrical data retrieval obtained by mechanical or another process should also have the provisions in the certificate has inferred above.

Relevant Sections of Indian Penal Code

The Indian Penal Code (IPC) is the principal criminal code of India that defines crimes and provides punishments for almost all kinds of criminal and actionable wrongs. The IPC extends to the whole of India except the states of Jammu and Kashmir and is an extensive law that covers all the substantive aspects of criminal law from nuisance at public places to murder, rape, dacoity, etc

The IPC came into existence in 1860 on recommendations of the first law commission of India established in 1834 under the Charter Act of 1833. The Code was made effective during the British rule in January 1, 1862 and was applicable to the whole of the then British India except the princely states as they had their own courts and legal systems till 1940s.
The Code was later adopted by the Independent India and Pakistan after partition. The Ranbir Penal Code applicable in Jammu and Kashmir is also based on this Code. It is applicable to all the citizens of India. The IPC has been amended numerous times since then and is now supplemented by various other criminal provisions. At present, the IPC is divided into 23 chapters and contains 511 sections in total.

RBI Act, 1934

This article comprises a detailed explanation of the RBI Act, 1934, the prologue of RBI Act, 1934, Issue functions of RBI Act and schedule and some important sections of the RBI Act, 1934.

The prologue of RBI Act, 1934

The prologue of the act mentioned the objective of RBI is to:

1. Set the matters of banknotes.
2. Set off the currency and credit system of the country to its benefit.
3. Keep the reserves with the view to security monetary firmness in India.

Issue functions

- The main key function of RBI is to issue banknotes, which was performed by the issue of the department which kept a full clear cut from the banking department.
- The torn or disfigured notes that can be exchanged in one of the functions are a matter of grace but not a matter of right in the RBI Act, 1934.
- Payment of stamp duty is not permitted on banknotes that RBI issues.
- The central government approves the design, form and material of book notes and gets a recommendation from the central board.

Second schedules of RBI Act, 1934

In the RBI Act, 1934, schedule banks are the banks that are listened to in the second schedule. Under this schedule, the banks should raise at least Rs 5 lakhs and capital. The banks added in the second schedule are known as scheduled banks, and these banks include scheduled cooperative banks and scheduled commercial banks. Scheduled banks comprise five non-similar groups, and scheduled commercial banks are urban cooperative banks and state cooperative banks.

Some important sections of the RBI Act 1943-

The RBI Act 1934 is of very much importance. There are many reliable sources on the internet that can be used to gather information about the same such as RBI Act 1934 pdfs. Also, the students appearing for competitive examinations can solve RBI Act 1934 MCQs available on the internet.

The important sections of the act are mentioned below:

Repo, reserve, derivative, money market instruments and securities are defined in section 45(u).

- Withdrawal of legal tender notes comes under section 26(2).
- Government businesses are transacted on agreement by RBI, and this comes under section 21A
- The business that RBI can carry outcome under section 17.
- Initiation and incorporation of reserve banks come under section 3.
- Demonetisation of notes comes under section 24.
- The re-issue of notes comes under section 27.

Law Relating To Employees And Internet

1. Although there are some gray areas in the laws surrounding employer responsibility for employee Internet and email use, companies can be liable. When employees use company resources or property to access the Internet, their actions can fall

back on the company. Therefore, it is a good idea for employers to have a clear policy on Internet and email use. It may also be wise to monitor employee use of company resources to avoid ongoing illegal behavior online.

Criminal Behavior

1. There are many online communications that may expose an employer to legal action depending on the circumstances. Activities like misuse of company email, violent threats, inappropriate comments or harassment may expose an employer to legal action. The liability for sexually and racially harassing someone via email or displaying inappropriate or pornographic websites at work may affect an employer, according to the Texas Workforce Commission (TWC). Accessing unauthorized websites and hacking computer systems can also lead to legal action.

Copyright Infractions

1. Almost every company has licensed software on its computers, which is protected from piracy by law. Employees who illegally copy or misuse software may land their employer in trouble. This is also true for the unauthorized use of pictures, information, logos and other materials found online. Additionally, illegal employee downloads of music or movies apply as well.

Privacy Laws

1. Employers usually hold a lot of private information about employees and the company itself on their sites. Leaking these items, such as medical records, can lead to violations of privacy laws.

Considerations

1. Determining liability for Internet use by employees is sometimes a murky issue. Under certain circumstances,

employers may be protected if they are unaware of employee activities on the Internet or email. Conversely, according to the article "Risky Business" found in the Shidler Journal of Law, Commerce and Technology, a court may also prove a company's "willful blindness" to an employee's online activities. These issues are relevant when an employee is using company property or a company network at work or at home. Additionally, legal actions have risen out of employee conduct on social networking sites.

Liability Protections

1. According to the TWC, the best way to avoid legal actions stemming from employee misuse of company computers, Internet or email is to have a clear policy on use and require employees to acknowledge the policy in writing. Also, an employer may want to exercise their right to electronically monitor employee Internet and email use. This should also be included in company policy and employees must know they will be monitored, with no expectation of privacy at work or when using company property.

Alternative Dispute Resolution

Alternative dispute resolution (ADR) refers to the different ways people can resolve disputes without a trial. Common ADR processes include mediation, arbitration, and neutral evaluation. These processes are generally confidential, less formal, and less stressful than traditional court proceedings.

ADR often saves money and speeds settlement. In mediation, parties play an important role in resolving their own disputes. This often results in creative solutions, longer-lasting outcomes, greater satisfaction, and improved relationships.

The New York State Unified Court System offers parties access to free or reduced-fee mediation and other ADR services in family law, general civil and commercial law disputes. These services are available in many courthouses and in the Community Dispute Resolution Centers located in almost all of New York State's 62 counties.

What is ODR?

Court-related **Online Dispute Resolution (ODR)** is a public facing digital space in which parties can convene to resolve their dispute or case.

Three essential components differentiate court-related ODR from other forms of technology-supported dispute resolution:

- The first is that the program operates exclusively online. In contrast to other court programs that provide an online interface with which to accomplish discrete tasks (e.g., e-filing, video

hearings), ODR users do not otherwise interact with the court for traditional in-court procedures or events.

- The second is that the program is explicitly designed to assist litigants in resolving their dispute or case, rather than a technology platform to support judicial or court staff decision-making. Dispute resolution inherently includes the potential to challenge the validity of claims or to raise affirmative defenses; court-related ODR is not merely a platform for defendants to negotiate a payment schedule to satisfy debts.
- Third, the program is hosted *or* supported by the judicial branch. It is not a form of private ADR, but instead integrates and extends dispute resolution services offered by the judicial branch into digital space to serve citizens efficiently, effectively, transparently, and fairly.

This definition of court-related ODR can encompass a variety of methods and tools to assist in dispute resolution. It can provide dispute resolution services without necessarily filing a formal complaint. It can support a variety of decision-making aids including discovery exchange; direct party-to-party settlement negotiations; synchronous or asynchronous mediation support; and technology-supported adjudication. When litigants successfully resolve their dispute, the program can populate standard settlement agreement forms that can be automatically filed with the court, if needed to dispose the case. If the litigants are unsuccessful, the program can also provide a seamless entry to the court's traditional dispute resolution by automatically populating and filing necessary court forms. The design and implementation of court-related ODR programs should not diminish due process or access to justice for program users.

Unit-4:

Electronic Business and Legal Issues

Evolution and development in E-commerce

Transcending boundaries and distance, e-commerce digitalized the world into a single platform, and, remarkably, e-commerce evolution only continues to accelerate.

From the initial spark in 1969 with the founding of Compuserve, e-commerce's story is one of astounding growth fueled by incredible innovation.

Three innovations are key to e-commerce growth:

1. **Personalization**: AI and machine learning made it possible to collate massive amount of data, make sense out of it and provide personalized shopping experiences. Feedback loops and dynamic adaptation to ever-changing consumer behavior enhance the whole customer experience.

2. **Omnichannel**: The rise of the internet enabled the emergence of social networks, which was further boosted by mobile devices. Social media is embedded in our daily activities. According to a Google report, almost 85% of the consumers begin their buying journey on one device and continue on another. That trend mandated seamless integration between online and offline sales channels.

3. **Secure payment**: Digital wallets and seamless electronic fund transfers have paved the way for a hassle-free payment experience. Paypal is the pioneer but Google Wallet, Apple Pay and many other mobile wallets are now on user devices. Increasingly, blockchain technology is making these transactions safer and faster.

4. **E-commerce evolution: B2C led the way**
5. In the early days, e-commerce was mainly driven on by the business to consumer business model, with retail as one of the early adopters. Apart from novelty, convenience played a major role in driving demand. Multiple players entered the field, intensifying the

competitive landscape. Companies started to distinguish themselves through wider product selection and more innovative services.

6. B2C e-commerce will continue to skyrocket. The global B2C e-commerce market, valued at USD 3.67 trillion in 2020, is expected to expand at a compound annual growth rate of 9.7% from 2021 to 2028. Growing digital dependency, the convenience of online shopping and a fast-growing digital population will drive growth.

Evolution of B2B e-commerce

The pandemic forced B2B companies, which preferred in-person sales, to look for more digital options. This gave rise to more B2B e-commerce solutions, which redefine buyer-seller interactions. B2B e-commerce is now much more transparent, efficient, and swift.

The market potential of B2B e-commerce is huge. Statista predicts B2B sales will reach $1.2 trillion by 2021. Globally, the B2B ecommerce market was worth $12.2 trillion in 2019, having grown from $5.8 trillion in 2013. Double-digit growth is predicted for B2B ecommerce sales through 2024.

E - Security

At e-Security System, we pride ourselves on the quality of our work. For years, we continually develop and improve our wide offer of state-of-the-art, tailor-made solutions and complete services in the range of Fire & Security Systems that makes our overall knowledge rank with the best in the industry.

We have been in business since 2005 and are approved by our esteemed customers as a professionally run organization with strong fundamentals and technological expertise meeting to all the highest recognized standards in the Fire & Security industry. Our competences, know-how and facilities allow us to implement projects which we create together with our customers to fully meet their individual expectations. We have been enriching knowledge and

competences by working on different sized projects across India. We offer our custom solutions to clients to help them design and structure their requirements.

E-Commerce and Taxation: Understanding the Difficulties

In just a decade of astounding growth, the Internet has reached a critical mass that is now attracting millions of consumers, and billions of their dollars, into a gigantic, ever-expanding virtual shopping mall. According to the figures published by VeriSign, which provides network security and authentication services to about 120.000 online retailers in the U.S., US$8.8 billion in online spending occurred during the period between the Thanksgiving holiday on Nov. 25 and the Monday after Christmas, Dec. 27, 2004. That constituted an increase of 24% compared to the same period in 2003. Not surprisingly, digital photograph equipment and entertainment were two of the fastest growing categories over the preceding year, with increases of up to 120% and 54% respectively. (1)

The magnitude of holiday season transactions in the U.S. clearly illustrates the potential of Internet commerce and how much this technology has been adopted by millions of consumers in the U.S. alone.

Tax systems, and particularly international taxation arrangements, can struggle to keep pace with globalization and market liberalization. Most of today's tax arrangements were developed in an era when tax authorities could rely upon Exchange controls, highly regulated capital markets and technological constraints to protect them from the negative fiscal effects of global activities. These barriers to cross-border activities protected tax authorities from the full implications of the interaction between national tax systems. While corporations globalized, tax authorities remained constrained by national frontiers.

However, today, the priority has to be to identify practical and reasonable ways of applying internationally accepted taxation norms to e-commerce; and, where necessary, of clarifying or developing

those norms. The key here is to maintain and strengthen the international dialogue. There are existing VAT principles and collection systems that can be readily applied when it comes to B2B (Business to Business) transactions whether they may be domestic or international. Done domestically though, B2C (Business to Consumer) transactions do not present much of a problem either; since transactions take place in a single territory.

What are Electronic Payments?

Electronic payments, or e-payments, are a way of making transactions or paying bills online or through an electronic medium, without the use of physical checks or cash. The most popular methods of electronic payments include credit cards, debit cards, virtual cards, and ACH (direct deposit, direct debit, and electronic checks). For example, when a vendor performs a service for your business and sends the invoice electronically, the process of paying the vendor via credit card, debit card, etc. is considered an electronic payment. With most electronic payment methods, the hard costs and fees associated with traditional B2B payments like checks are no more — including paper, postage, and manual labor expenses.

The Benefits of E-Payments

Electronic payments and e-payments systems are highly beneficial to both businesses and their suppliers. In the context of accounts payable, e-payments are a win-win in that they reduce costs, improve relationships, increase visibility and provide enhanced security when compared to traditional checks. Here's how:

- **Lowered Processing Costs:** The more payments a business can process electronically, the less they spend on paper and postage, along with the time required to print, sign, stuff, and mail checks. In fact, shifting to a holistic e-payments strategy can reduce payment processing costs up to 80 percent.

- **Strengthened Supplier Relationships:** Businesses can improve vendor relations by facilitating quicker, more secure payments that include rich remittance data for easier reconciliation.
- **Increased Payment Security**: Electronic payments are inherently more secure than paper checks, and specific methods like virtual cards offer even greater protection against fraud. On top of that, best-in-class e-payment systems include additional features and controls to help secure the payments process.
- **Enhanced Visibility:** E-payment systems provide your business with greater visibility into payment statuses, financial metrics, and accurate audit trails. They additionally reduce the costs and probability of data entry mistakes.

Types of Electronic Payments

While there are many different types of electronic payments, here are the most common categories that make up the majority of e-payments.

- **Card Payments:** Credit and debit card payments are the most common type of electronic payments. Despite their decreasing popularity among younger generations, credit card payments continue to be the most utilized electronic payment form due to their rewards and rebates offerings.
- **Bank Transfer Payments:** A bank transfer is when funds are moved from one bank to another and can be done in a few different ways. Most bank transfers are conducted via direct deposit, where payments are deposited electronically into the recipient's bank account. However, in the U.S., bank transfers are conducted with ACH transfer payments.
- **Virtual Card Payments:** A virtual card is a randomly-generated 16-digit number that can only be used for the specified amount and can only be charged a single time.

Because of this, virtual cards ensure secure payments that are impossible to decrypt.

- **Cross-Border/FX Payments:** FX payments and cross-border payments allow businesses to send and receive money internationally. This process is conducted via wire transfers, forward contracts, cross-currency transactions, and more. This is especially useful for businesses working with international customers and suppliers.

What Is a Supply Chain?

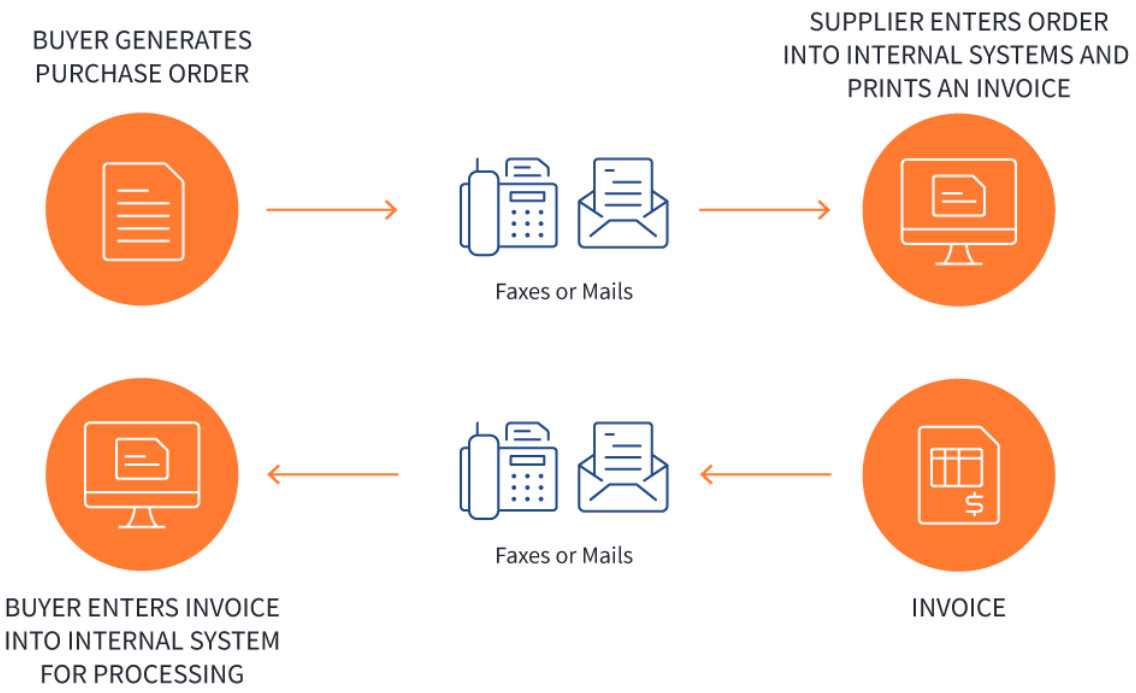
A supply chain is a network of individuals and companies who are involved in creating a product and delivering it to the consumer. Links on the chain begin with the producers of the raw materials and end when the van delivers the finished product to the end user.

Supply chain management is a crucial process because an optimized supply chain results in lower costs and a more efficient production cycle. Companies seek to improve their supply chains so they can reduce their costs and remain competitive.

What is Electronic Data Interchange (EDI)?

Electronic Data Interchange (EDI) is the electronic interchange of business information using a standardized format; a process which allows one company to send information to another company electronically rather than with paper. Business entities conducting business electronically are called trading partners.

Many business documents can be exchanged using EDI, but the two most common are purchase orders and invoices. At a minimum, EDI replaces the mail preparation and handling associated with traditional business communication. However, the real power of EDI is that it standardizes the information communicated in business documents, which makes possible a "paperless" exchange.



Electronic Market(e-Market)

An electronic market is an inter-organizational information system they allow the participating buyers and sellers to exchange information about prices and product offerings. The firm operating the system is referred to as the intermediary, which may be a market participant- a buyer or seller, an independent third party, or a multi-firm consortium.

Electronic markets are the foundation or of electronic commerce. They potentially integrate advertising, product ordering, delivery of products, and payment systems. Many electronic markets also offer additional services, such as payment or logistics services that help members complete a transaction. They may also support community activities like distributing industry news, sponsoring online discussions, and providing research on customer demand or industry forecasts for components and raw materials.

Functions of E-Markets:-

E-markets serve three particular functions:

1. **They act as an exchange for business transactions-not only purchasing but also for checking price and stock availability, invoicing and order chasing.**
2. **They manage catalog content, converting product information into a common format understood by all parties.**
3. **They provide additional services to support the trading process such as shipping, payment, tendering and determining a company's financial status.**

Emerging Trends

We are currently going through one of the most significant historical changes ever experienced in the last 100 years. Old businesses will change and new businesses will emerge. We are already seeing a shift in services our clients are adopting as a response to this pandemic. Essential services in relation to healthcare, energy and natural resources, water, and emergency services will continue to be in demand, although the business models for these industries may change.

We need to be vigilant and cautious about the further impact of the spread of the virus, and resilient to create new ways of living and working. We need to gain inspiration on how two of the most populous nations of the world; India and China are managing the

situation. The collective wealth of western nations will help repurpose spending and improve healthcare.

New ways of living and working will emerge as soon as fear subsides, so let's start now, by discussing ten ways to reimagine and reinvent our lives, our organisations and our society.

1. Globalisation will be redefined with a stronger emergence of social capitalism

The unregulated and free-market globalisation may gradually come to an end due to COVID-19 exposing the serious risks of independent and uncoordinated actions of countries on the global economy and the well-being of people. The pandemic proved that issues arising in one country has a domino effect and can end up having a serious impact on the entire economic world.

A new form of globalisation that recognises interdependence and the good of humanity based on collective actions of countries, businesses and people will start to emerge. As a result, companies will change their governance and business management models with greater focus on corporate social responsibility and the well-being of people. Many countries will pass new laws to protect employees in situations such as COVID-19. With the emergence of social capitalism, a new kind of capitalism will drive companies. Not only markets and market regulation, but also what is good for the communities and the society, will drive business strategy.

2. Acceleration of digital transformation

The notion of digital transformation is now fairly advanced with many organisations working on transforming businesses over the last two years, if not more. COVID-19 will force companies to take radical steps to adopt technology advancements, and modernise culture, organisational structures, measurement systems and operating architectures.

There is common agreement among top business leaders that even if the organisation is ahead today, they have to be continually prepared to change, take calculated risks and be prepared to fail fast, or their business is likely to get disrupted. Therefore, accelerating digital transformation journeys would become a top priority for many companies to ensure business continuity, improve productivity and launch new business models to remain competitive.

3. The use of an on-demand workforce will increase

With the economic impact of COVID-19, companies and people will embrace technology enabled on-demand workforce models and platforms. This would improve workforce planning, financial management and access to diverse skills. Companies should understand and learn how to engage and retain on-demand talent with improved People Management programs, strategies and tools to make value for and on-demand workforce.

4. A new burning platform for healthcare reform

COVID-19 has exposed major gaps in the healthcare systems of some of the most advanced countries of the world. The pandemic has created a burning platform for healthcare reform in the United States, United Kingdom, France and many developing nations. COVID-19 will force the healthcare industry to transform and provide care that is more equitable. This will create new opportunities for many, who are involved in building the new system.

Other than industry reform, companies will need to make efforts to concentrate on individuals' healthcare. The need for emotional connectivity will increase as remote working, social isolation and social distancing practices become more common. Companies will increase focus on employee's mental health and well-being, to avoid the downside of limited in-person human contact.

5. Supply-chains will fragment and reconfigure themselves

Supply chains will fragment further with technology platforms integrating them. Multi-tier supply-chains will emerge and track critical components including the origin of supply and incremental value-adds. This would open exploration of new ways to engage with customers, manage inventories, optimise production and distribution, logistics management and managing cash/capital.

As well as this, as 5G internet becomes more widely available, it will increase the use of online internet systems and consequently reduces the risk of too much centralisation. Traditional business strategy relies on market boundaries and competitors. In the post COVID-19 era, companies need to create new breakthrough value for their customers continuously, not just once. Unless companies embrace global thinking, and establish strategic alliances and partnerships with others in a global ecosystem, not just local, value creation will become very challenging in a rapidly changing business environment.

6. The definition of 'workplace' will change

The current remote working arrangements, if continued for more than three months, could permanently shift working patterns. New norms will be established for these working conditions, redefining work life and personal life boundaries. The workplace will no longer be simply an office where people come to each day, and leave to go home each night. With major changes on the horizon, a need to reimagine the purpose of a workplace will arise. Increasingly, workplaces will become collaboration hubs to achieve common objectives, compared to just providing a place for people to work. Unnecessary overhead costs such as travel will be cut back, leaving no option but to enforce virtual interactions replacing physical face-to-face meetings.

7. Industries will be forced to reinvent with upskilling and reskilling becoming a major priority

COVID-19 has accelerated the disruption of many industries that many pundits have been predicting for years. Almost all industries, including airlines, retail, hospitality, healthcare, education, construction and technology, will require rapid transformation to their business models in order to remain viable. New business models and value-chains will significantly increase a need for new skills.

Last year, the **WEF warned of a major disruption** in the labour markets of 15 developed and emerging countries that would lead to a net loss of over 5 million jobs and the emergence of millions of new jobs. COVID-19 is already seriously affecting the labour markets. Therefore, to minimise emerging unfavourable social and economic impact, reskilling and upskilling of the workforce will become a top priority of many companies. The education and training systems will need to go through a major shake-up to help the workforce quickly reskill and upskill using virtual solutions. Human-centric technology adoption will become important to ensure communication and knowledge streams remain existent.

8. Change in work habits will lead to urban transformation

With the changing landscape of business operations, the cost of commercial real estate will fall to coincide with the reduced demand. Once remote work becomes more of the norm, the need for corporate complexes diminishes but will open up new ways of utilisation, whether it is space sharing, event hire or a collaboration venue. Along with many other trends, COVID-19 has accelerated the move for commercial real estate to become more adaptable, allowing industries to be reborn and rethink their place in their evolving surroundings.

9. Rapid innovation will keep businesses afloat

Technology will continue to drive innovation across business models in various industries, allowing new businesses to enter the market and disrupt incumbents in serious ways. In order to drive business growth, stay relevant in changing times, and differentiate from the competition, business leaders must be able to think creatively and embrace innovation to create break-through value for their customers. In the post COVID-19 era, there will be a greater need to increase innovation and move away from the comfort of operating 'business as usual'. If organisations do not adapt to new ways of working they may experience an existential crisis.

The Importance of Cyber Law

Cyberlaw is used by smaller business organizations which are extremely vulnerable because of the ineffective cybersecurity. It is very important to all types of business organizations, particularly when you think about the importance or advantages of the internet as well as digital systems are for your day-to-day operations. There are various reasons for which Cyber Law, is very important, are listed below;

- **It allows employees to work safely** – with the help of cyberlaw, you and the employees of your company haven't got any risk from a potential cyberattack. If your system becomes infected than that can really hamper their productivity.
- **It can protect your business** – This is one of the biggest factors, because of which cyber law is very important. It allows the employees to surf the internet as and when they require it. You have to ensure that they can't at risk from potential threats.
- **It protects the personal information of the user** – One of the most important factors in the digital world is to keep your personal information secret. It is very essential for the customer that they are quite capable of selling the information.
- **It protects productivity** – There are many viruses present which can slow down your personal computer. It may often bring your personal business to a standstill.

Significance of cyber Ethics

Cyberethics is a branch of computer technology behavior that defines the best practices that must be adopted by a user when he uses the computer system. In simple terms, cyberethics refers to the basic ethics and etiquette that must be followed while using a computer system. Ethics, in general, refers to propagating good behavior, similarly by cyber ethics we refer to propagating good behavior online that is not harsh or rude. Cyberethics governs rules that individuals must be polite and responsible when they use the internet. Cyberethics aim to protect the moral, financial, social behavior of individuals. Cyberethics engages the users to use the internet safely and use

technology responsibly and sensibly. Cyberethics empathizes the behavior that must be adopted while using cyber technology.

Some of the breaches of cyberethics are listed below:

- **Cyber Bullying:** Cyber Bullying is a form of bullying carried out via internet technology such as social media where individuals are mocked on their physical appearance, lifestyle, preferences, etc. The teenage generation or say youngsters are the major victims of this form of cyber ethic breach. Cyberbullying affects the emotional ethics of individuals and can cause mental disturbance to individuals.
-
- **Hacking:** Stealing a user's personal or organizational information without authorized permission is not considered a good practice. It is one of the riskiest cyber breaches to data leak. Data leak includes passing of sensitive information such as passwords, bank details of the user to a third-party user who is not authorized to access the information.
-
- **Copywriting:** Claiming of another individual as one's own is another type of cyber ethic breach that must be eradicated. Never engage in copywriting another person's content or document and claim as it is your own. It leads to a serious problem called plagiarism, which is a punishable offense and considered a legal crime. It is always advisable to follow general cyberethics, while using the internet or say any kind of technology. A proper code of conduct must be followed while using cyber technology. Cyberethics if not used wisely can lead to serious situations. Social and legal laws are defined to use cyber technology wisely. In extreme cases, legal action can be taken if there is a violation of cyber ethics.

Need for Cyber regulations and Ethics

The main objective of the technology is to provide a sense of security to the users. But nowadays, with the improvement of technology due to cyber crimes and ethics, day-to-day activities have become much more easier and user friendly. It has led to a harsh world of security threats at the same time by agencies like hackers, crackers etc. Hence a number of information technology methods have come up to curb such destructive and dangerous activities to achieve the real objective of such improved technology, i.e., to provide a sense of security to the users. Some measures to curb cyber crimes via cyber law and ethics are as follows:

- Synchronised passwords

Passwords are meant for one`s security. The password synchronised on the card changes after every 30-60 seconds which makes it valid for one-time log-on sessions only. Other methods providing security are fingerprint identification, signature, voice, retinal identification and biometric recognition etc to impute password and pass phrases.

- Encryption

This is an important tool to protect data in transit. Plain content (readable) can hence be changed over to cipher text (coded language) by this technique and the beneficiary of the information can decode it by changing over it into plain content again by utilizing private key. With the exception of the beneficiary whose holder of the private key unscramble the information, nobody can access sensitive data.

The data in travel, as well as the data put away on PC, can be secured by utilizing Conventional cryptography technique. Regular issue lies during the appropriation of keys as anybody who catches it or captures it can make the entire object of encryption to stop. Open key cryptography was one answer for this where the open key could be

known to the entire world however the private key was just known to the recipient, it is extremely hard to get a private key from an open public key.

- Firewalls

It divides between the framework and potential interlopers or intruders to shield the arranged archives from spilled or got to. It would just give the information to stream access PCs which in this way are perceived and confirmed by one's framework. Therefore, it just allows access to the framework to ones previously registered with the PC.

- Digital signatures

Advanced or Digital Signature made by utilizing methods for cryptography by pplying algorithms. This has its unmistakable use in the matter of banking where client's mark is accordingly distinguished by utilizing this technique.

Ethics in Information society

The principles on which information ethics are based derive from the Universal Declaration of Human Rights(link is external) and include the right to freedom of expression, universal access to information, the right to education, the right to privacy and the right to participate in cultural life. Promoting values and principles based on fundamental human rights is central for the development of an equitable information society and raising awareness about ethical issues related to information is one of the six priorities of the Information for All Programme (IFAP).
Read less
One of the challenging ethical issues that IFAP addresses is the use of cyberspace for the radicalization of young people leading to violence. Interventions are articulated around the support of multidisciplinary research, empowering youth online communities

and key youth stakeholders, strengthening mobilization and cooperation between media professionals and practitioners and supporting creative media campaigns and outreach strategies targeting policy-makers and opinion-makers as well as the general public.

Attention is also given to the ethical dimensions of Artificial Intelligence that can certainly contribute towards sustainable development, but also pose questions related to the use of this emerging technologies and the respect of fundamental human rights. UNESCO is playing a leading role to sensitize different stakeholders on the ethical dimension of the use of Artificial intelligence and reflection on challenges to be addressed and the development of its use in furthering inclusive equitable knowledge societies. World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) is also playing a leading role on ethical questions raised by artificial intelligence.

Introduction to Artificial Intelligence Ethics

The course introduces the fast evolving interdisciplinary research area of Artificial Intelligence (AI) Ethics to doctoral students who are interested in either AI as a computer science discipline or students interested in researching the societal and personal impact of AI technologies introduced in society.

The course consists of **7 modules**.

The first two modules establish a common foundation for following the course.

The first introductory module presents AI as a technical discipline, the main methodology and research questions. The second module offers an introduction to artificial intelligence studies in social sciences and organisational studies.

In module 3 the students learn the foundations and state-of-the-art in accountability and transparency of AI. They get an entry point to research

in this area: learn how to learn more and how to engage with that research community.

In module 4 the students will learn what the basic problems and approaches are to making algorithms explainable. They will understand the difference between explainability and interpretability of algorithms and how transparency relates to these concepts. The students learn to compare and evaluate different ML algorithms with respect to their explainability.

In module 5 the students will learn what the concept of fairness means with respect to algorithms. They will learn to recognise the different definitions of fairness, their motivation, strengths and weaknesses. the students will be introduced to the basic methods for mitigating bias in algorithms and data (preprocessing, in-processing and post processing).

In module 6 the students learn the role that privacy concerns play in artificial intelligence. In particular they will be introduced to the basic principles and methods of ensuring differential privacy and data.

Module 7 is reserved for discussing open research problems in AI ethics, challenges and possible approaches.

Each module consists of 4x45 minutes. Lectures are combined with hands-on exercises for the students and discussions. Reading assignments will be assigned between each module.

Ethical Issues in AI and core Principles

There are numerous accounts of the ethical issues of AI, mostly developments of a long-standing tradition of discussing ethics and AI in the literature (Coeckelbergh 2019, Dignum 2019, Müller 2020), but increasingly also arising from a policy perspective (High-Level Expert Group on AI 2019). In this book and the SHERPA project[2] that underpins much of the argument, the aim was to go beyond literature reviews and find out empirically what people have in mind when they speak of the ethical issues of AI. I will focus here on ten case studies and the open-ended first stage of a Delphi study to

come to a better understanding of how the ethics of AI is perceived by people working with and on AI systems.

The level of analysis of the case studies was defined as organisations that make use of AI. Case studies are a methodology that is recommended to provide answers to the “how” and “why” of a phenomenon and events over which the researcher has little or no control (Yin 2003a, b). In order to gain a broad understanding, a set of application areas of AI was defined and case study organisations identified accordingly. Using this methodology, the case studies covered the following social domains:

- employee monitoring and administration
- government
- agriculture
- sustainable development
- science
- insurance
- energy and utilities
- communications, media and entertainment
- retail and wholesale trade
- manufacturing and natural resources

For each case a minimum of two organisational members were interviewed, the aim being to engage with at least one technical expert who understood the system and one respondent with managerial or organisational expertise. Overall, for the ten case studies, 42 individuals were interviewed. Based on the initial draft report of each case, peer review among the research team was undertaken, to ensure that the cases were consistent and comparable. For a detailed overview of the methods, findings and outcomes of the case study research, see Macnish et al. (2019).

Introduction to Block chain Ethics

Blockchain's ethical issues for organizations stem from its three main promises: immutability, disintermediation (distributed verification), and automation. Immutability results in the permanency of a human past record and raises ethical issues such as privacy and transparency concerns (Hofmann et al., 2017). Disintermediation refers to horizontal decision-making and the numerosity of stakeholders in verifying outcomes (Quiniou, 2019). Disintermediation raises ethical issues related to accountability and equal opportunity. Automation refers to the self-executing features of coded agreements called smart contracts (Szabo, 1996) which raises issues related to human dignity among others.

This paper is among the first to map out DePo at various phases of people operations. First, this paper brings light to privacy challenges for the entry and exit stages of people operations while arguing that contractarianism—based on a hypothetical *ex ante* contract—can best capture the associated ethical issues. As for intraorganizational affairs, the paper offers fresh views of blockchain's potential impacts on compensation, shared leadership, conflict management, and performance evaluation. It suggests that each of the applications requires separate ethical analysis. For instance, on shared leadership and a new form of conflict management—what we call *distributed conflict management* (DCM)—virtue ethics with its focus on human flourishing best captures the associated ethical nuances. From a broader perspective, this paper contributes to the existing literature by showing how emerging technologies can foster the transition from the purely utilitarian view of human resources to a more collaborative environment. In achieving so, the paper analyzes the ethical ramifications of emerging technologies which requires in-depth understanding of their disruptive potentials and a more robust stage-by-stage analysis that is not merely related to the consequences of emerging technologies.
Theoretical Background

A New Kid on the Block

Blockchain technology is a new form of trust and choice architecture, which allows for the disintermediation of third parties (Werbach, 2018). At the heart of blockchain technology is a new form of "consensus" that makes it possible for the platform and users to make decisions without oversight and presence of a third party. For example, if person A is transferring a sum of money from her account to person B, banks record the transaction. In blockchain and crypto-economics, other users of the platform record the transaction. By multiplying the ledgers that include the transaction, blockchain makes it extremely difficult for a single user or even a group of users to manipulate the transaction or double-deal. The blockchain platform often includes an incentive mechanism to encourage users to participate in the record-keeping process. Most notably, in

the Bitcoin platform, the users are rewarded if they solve complex mathematical problems (called mining) (Böhme et al., 2015). In essence, blockchain is a crowd-based or peer-to-peer platform, which enables verification and storing of information with the help of all of its users (i.e., disintermediation). The information is stored in digital blocks, which creates a chain of immutable information (Tapscott & Tapscott, 2017).

Blockchain enables a new network-based decision-making process whereby users are not merely the recipients of information of decisions but also the decision-makers (Ghodoosi, 2021). Put differently, at its core, blockchain enables the creation of *value* through a consensus-based verification mechanism based on an incentive structure. Values, therefore, are created not by trust in a government (e.g., dollar) but based on verification of others (Tapscott & Tapscott, 2017). Moreover, in blockchain platforms, users are often anonymous or pseudonymous which enables a new form of engagement with the network and a new type of decision-making (Aitzhan & Svetinovic, 2016). Even though the technology is still in a nascent phase relative to other technologies, blockchain's promise lies in its new form of rendering organizational decisions that can change the structure of organizations.

The Power of Artificial Intelligence and Blockchain

The relationship between blockchain and AI is evolving. Blockchain is a record mechanism enabling distributed decision-making and immutable record keeping. However, the information that is fed into the blockchain system and ultimately printed into the blocks in a blockchain can be AI-enabled. In other words, AI is the connection between blocks and the external data. For example, imagine a blockchain-based distributed ledger social network. All users' public information is stored on blocks. However, new blocks can be added based on AI algorithms which collect the information of users (e.g., about their preference for a presidential candidate) and store them into new blocks. One difference between the distributed social network and the existing one is that AI algorithms allow for further decentralization (elimination of central planning) as the AI algorithms determine the information that is shared among users and added to new blocks. One can further imagine that both the AI algorithm and the types of information recorded can be modified pursuant to the consensus mechanisms (similar to a constitution) adopted as the underlying basic logic of this social network. The use of blockchain jointly with AI in organizations presents novel ethical questions given that the immutable data storage capability of blockchain meets the ever-increasing capability of AI in generating data.