CYBER LAWS AND SECURITY POLICIES

M.RK.CHAITANYA

ASST.PROFESSOR

DEPARTMENT OF CSE

What is Cyber Law?

- Cyber law, also known as Internet Law or Cyber Law, is the part of the overall legal system thet is related to legal informatics and supervises the digital circulation of information, e-commerce, software and information security. It is associated with legal informatics and electronic elements, including information systems, computers, software, and hardware.
- It covers many areas, such as access to and usage of the Internet, encompassing various subtopics as well as freedom of expression, and online privacy.

What is Cyber Law?

What is Cyber Law?

- Cyber laws help to reduce or prevent people from cybercriminal activities on a large scale with the help of protecting information access from unauthorized people, freedom of speech related to the use of the Internet , privacy, communications, email, websites, intellectual property, hardware and software, such as data storage devices.
- As Internet traffic is increasing rapidly day by day, that has led to a higher percentage of legal issues worldwide.
- Because cyber laws are different according to the country and jurisdiction, restitution ranges from fines to imprisonment, and enforcement is challenging.

What is Cyber Law?

- Cyberlaw offers legal protections for people who are using the Internet as well as running an online business.
- It is most important for Internet users to know about the local area and cyber law of their country by which they could know what activities are legal or not on the network.
- Also, they can prevent ourselves from unauthorized activities.

What is Cyber Law?

- The Computer Fraud and Abuse Act was the first cyber law, called CFFA, that was enacted in 1986.
- This law was helpful in preventing unauthorized access to computers.
- And it also provided a description of the stages of punishment for breaking that law or performing any illegal activity.

Why are cyber laws needed?

- There are many security issues with using the Internet and also available different malicious people who try to unauthorized access your computer system to perform potential fraud.
- Therefore, similarly, any law, cyber law is created to protect online organizations and people on the network from unauthorized access and malicious people.
- If someone does any illegal activity or breaks the cyber rule, it offers people or organizations to have that persons sentenced to punishment or take action against them.

What happens if anyone breaks a cyber law?

- If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law.
- There are many situations like if you break the law on a website, your account will be banned or suspended and blocked your IP (Internet Protocol) address.
- Furthermore, if any person performs a very serious illegal activity, such as causing another person or company distress, hacking, attacking another person or website, advance action can be taken against that person.

Importance of Cyber Law

- Cyber laws are formed to punish people who perform any illegal activities online.
- They are important to punish related to these types of issues such as online harassment, attacking another website or individual, data theft, disrupting the online workflow of any enterprise and other illegal activities.

Importance of Cyber Law

- If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law.
- It is most important to punish the criminals or to bring them to behind bars, as most of the cybercrimes cross the limit of crime that cannot be considered as a common crime.

Importance of Cyber Law

- These crimes may be very harmful for losing the reliability and confidentiality of personal information or a nation.
- Therefore, these issues must be handled according to the laws.

Areas involving in Cyber Laws

- These laws deal with multiple activities and areas that occur online and serve several purposes.
- Some laws are formed to describe the policies for using the Internet and the computer in an organization, and some are formed to offer people security from unauthorized users and malicious activities.
- There are various broad categories that come under cyber laws; some are as follows:

Areas involving in Cyber Laws

Fraud

- Cyber laws are formed to prevent financial crimes such as identity theft, credit card theft and other that occurring online.
- A person may face confederate or state criminal charges if he commits any type of identity theft.
- These laws have explained strict policies to prosecute and defend against allegations of using the internet.

Areas involving in Cyber Laws

Copyrighting Issues

- The Internet is the source that contains different types of data, which can be accessed anytime, anywhere.
- But it is the authority of anyone to copy the content of any other person.
- The strict rules are defined in the cyber laws if anyone goes against copyright that protects the creative work of individuals and companies.

Areas involving in Cyber Laws

Scam/ Treachery

- There are different frauds and scams available on the Internet that can be personally harmful to any company or an individual.
- Cyber laws offer many ways to protect people and prevent any identity theft and financial crimes that happen online.

Online Insults and Character Degradation

- There are multiple online social media platforms that are the best resources to share your mind with anyone freely.
- But there are some rules in cyber laws if you speak and defaming someone online.
- Cyber laws address and deal with many issues, such as racism, online insults, gender targets to protect a person's reputation.

Online Harassment and Stalking

- Harassment is a big issue in cyberspace, which is a violation of both criminal laws and civil.
- In cyber laws, there are some hard laws defined to prohibit these kinds of despicable crimes.

Data Protection

- People using the internet depends on cyber laws and policies to protect their personal information.
- Companies or organizations are also relying on cyber laws to protect the data of their users as well as maintain the confidentiality of their data.

Contracts and Employment Law

- When you are visiting a website, you click a button that gives a message to ask you to agree for terms and conditions; if you agree with it, that ensures you have used cyber law.
- For every website, there are terms and conditions available that are associated with privacy concerns.

Trade Secrets

- There are many organizations that are doing online businesses, which are often relying on cyber laws to protect their trade secrets.
- For example, online search engines like Google spend much time to develop the algorithms that generate a search result.
- They also spend lots of time developing other features such as intelligent assistance, flight search services, to name a few and maps.
- Cyber laws help these organizations to perform legal action by describing necessary legal laws for protecting their trade secrets.

How to protect yourself on the Internet

- Although the Internet is a resource that contains multiple different types of content, there are many hackers or unauthorized users that may be harmful to you in order to thief your personal information.
- Below are given all of the steps that may help you to keep your personal information and computers safe while using the Internet.
- All of the given steps or suggestions can be beneficial for all computer users, even if what type of computer, device, or operating system they are using.

How to protect yourself on the Internet

How to protect yourself on the Internet

- Verify data is encrypted
- When you are sending any confidential information, such as debit card numbers, credit card numbers, usernames, or passwords, send these types of information securely.
- In Internet browsers, look for a small lock (Internet browser security lock) to verify this; an icon will be shown in the right corner of the bottom of the browser address bar or browser Window.
- If you see the icon, it should be in a locked condition and not in an unlocked position.
- Also, make sure the URL starts with https (Hypertext Transfer Protocol Secure), as displaying in the below screenshot:

How to protect yourself on the Internet

Internet Explorer secure address bar.

- If the lock icon is in the locked position and data is intercepted, the data is encrypted that helps to keep secure your data and prevent others to understand it.
- The data can be read by anyone if the lock is in the unlocked position or no lock is visible because all information will be in the form of plain text.
- For example, an online forum is not secure, use a password, but you will not use the password with protected sites like an online banking website.

Use a safe password

- Like online bank site or other websites that contain confidential information, need to use very strong passwords, it is also recommended; you must use the different and strong password for all websites that require login id and password.
- You could use a password manager if you required help to remember your password.

Keep your software and operating system up-to-date

- To protect yourself on the Internet, it is better to update your software installed on your computer and operating system regularly.
- It is necessary because many updates are released by the developers of the operating system that are related to computer security-related issues.
- Therefore, you should update your system when the latest updates are released.

When available always enable two-factor authentication

- You can use the two-factor authentication feature to make more secure your accounts, like Gmail or others that require a login and contain your private data.
- It offers advanced protection by adding an additional step in verifying you at the time of login.
- If you enable two-factor authentication and the service does not verify your computer or other devices after authenticating your password, it sends a text message with a verification code on your cell phone.
- It includes more powerful security; for example, if someone knows your password of any account and tries to access your account, but he does not have your phone, he cannot access your account even with a valid password.

Always be cautious of e-mail links and attachments

- The email attachments and hyperlinks sent through email are the most common resources to spread viruses and malware.
- It is recommended to always be extremely cautious to open any attachments and hyperlinks, which you have received through email from others, even if they have sent by friend or family.

Evolution of Computers

Introduction

- We all use computers in our daily lives for a variety of reasons. Computers are now portable and affordable, but once, there was a time when a computer used to take up an entire room's space, and only a few of them existed in this world.

Evolution of Computers

Abacus (c. 2700 BC)

- When you were kids, you must have owned an abacus on which you learned basic mathematical skills.
- Did you know that the abacus originated in ancient Mesopotamia and is one of the earliest known computing devices?
- It consisted of beads on rods and was used for basic arithmetic calculations.

Evolution of Computers

First Generation – Vacuum Tubes (1940 – 1956)

- Did you know that the 1930s marked the beginning of calculating machines, considered the first programmable computers? Who knew that computers were this old?
- Konrad Zuse created what became known as the first programmable computer, the Z1, in 1936 in his parent's living room in Berlin.
- You can see in the picture below just how gigantic the computer was.

Evolution of Computers

- The 1940s saw the emergence of electronic computers, including the ENIAC (Electronic Numerical Integrator and Computer) and the EDVAC (Electronic Discrete Variable Automatic Computer).
- These machines used vacuum tubes and punched cards for data processing. In the picture attached below, you can see a scientist using ENIAC for computational purposes.

Evolution of Computers

Second Generation – Transistors (1956 – 1963)

- In 1947, the invention of the transistor by Bell Labs revolutionized computing. Transistors replaced bulky vacuum tubes, making computers smaller, faster, and more reliable.
  101
- Second-gen computers still count on punched cards for input/printouts. In the above image, you can see two computer engineers working on a computer transistor.

Evolution of Computers

- The language emerged from a binary language to a symbolic (‘assembly’) language. This meant programmers could discover instructions in words.
- Until 1965, computers were only used by mathematicians and engineers in a lab setting. Programma 101 changed everything by offering the general public a desktop computer that anyone could use.
- The 65-pound machine was the size of a typewriter and had 37 keys and a printer built-in.

Evolution of Computers

Third Generation – Integrated Circuits (1964 – 1971)

- Third-generation computers started using integrated circuits instead of transistors.
- Do not get overwhelmed by the new vocabulary! Just know that IC is a hardware component of a computer.
- Technically, the integrated circuit (IC) is a semiconductor material that contains thousands of transistors.

Evolution of Computers

- Because of IC, the computer becomes more reliable and fast, requires less maintenance, is small in size, is more affordable, and generates less heat.
- You can see in the image above how multiple IC racks are used to power a computer.

Evolution of Computers

Fourth Generation – Microprocessors (1972 – 2010)

- Intel's 4004 microprocessor marked a pivotal moment in computing history.
- It was the world's first commercially available microprocessor and laid the groundwork for the personal computer revolution.

Evolution of Computers

- **World Wide Web (1991)**

❖Tim Berners-Lee's invention of the World Wide Web revolutionized communication and information access.

❖The web made the internet user-friendly and accessible to the masses.

Evolution of Computers

- **Mobile Computing (2000s-Present)**

❖The advent of smartphones and tablets transformed computing into a complete mobile experience, with powerful handheld devices becoming integral to daily life.

Evolution of Computers

Fifth Generation – Artificial Intelligence (2010 Onwards)

- This is the computer generation that we use.
- We know that computer devices with artificial intelligence technology are still in development.
- Still, some of these technologies are emerging and being used, such as voice recognition or ChatGPT.
- AI is an authenticity made possible by adopting parallel processing and superconductors.
- In the future, computers will be revolutionized again by quantum computation, molecular, and nanotechnology.

Evolution of Computers

- In 2019, Google claimed to have achieved “quantum supremacy” by performing a calculation on its quantum computer that would take even the most advanced classical supercomputers thousands of years to complete.
- Today’s most innovative computers are tablets and iPads, which are simple touchscreens without a keyboard, mouse, or a separate CPU.

Meaning And Definition Of Cyber Space

- The term ‘cyberspace’ was first coined by William Gibson in his 1982 short story ‘Burning Chrome’ to refer to a computer-generated virtual reality.
- However, the term became popular in 1984, after its use in Gibson’s novel Neuromancer.
- Etymologically, cyberspace is a compound word and the origin of the first term ‘cyber’ comes from the Greek word Kubernetes, which means pilot, governor, and ruler.
- The root ‘cyber’ is also related to ‘cyborg’; a term that describes a human-machine synthesis resulted from connecting the human body in advanced high-tech devices.
- According to Gibson, cyberspace is the name of a real non-space world, which is characterized by the ability for the virtual presence of, and interaction between, people through icons, waypoints and artificial realities’. However, it is difficult to give concise definition to cyberspace as computer network and its service is increasing day by day.

Cyber Crime In India

- With the increase in a virtual environment, cyber-crimes are also increasing.
- Whenever we think about cyberspace the first thing that comes to our mind is cybersecurity.
- Various measures are being taken by Governments and companies in order to prevent these cybercrimes.
- At the present time securing the data has become one of the biggest challenges in cyberspace.

Cybercrimes Against Person

- The Cybercrimes committed against a person and directly affect the individual.
- The theft of personal information of individuals and misuse of them.
- It includes various crimes such as Cyber harassment, cyberstalking, child pornography, social engineering, etc.
- Cyber harassment is distinct cybercrime that is commit in cyberspace.
- Harassment can be racial, social, sexual, or religious.
- Cyber harassment as a crime has resulted in the violation of the privacy of citizens.
- When the privacy of online citizens is violated it results in cybercrime of great nature.

Cybercrimes Against Property

- This second category of cybercrimes is commit against all forms of property.
- These crimes include computer vandalism (deliberately damages others' property) and transmission of harmful viruses or programs.
- A Mumbai-based start-up engineering company lost much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of corporate cyber spy software.
- Certain offenses which affect a person's property are Intellectual property crimes, cybersquatting, cyber trespass, hacking, etc.

Cyber Crimes Against Government

- This third category of cybercrime is commit against the government, and nation's sovereignty is affect.
- It is also known as cyber terrorism when an individual or group of people "cracks" into a government or military maintain website.
- It alsoincludes hacking, accessing confidential information, cyber warfare, etc.
- For example Mumbai attack 26/11 was cyber terrorism.

Cyber Crimes Against Society

- This fourth category of Cybercrime is committed against people at large, it affect large number of people living in such as Child pornography, Bank thefts, Online gambling etc.

Cyber Jurisprudence

- Cyber Jurisprudence describes the principles of legal issues, which exclusively regulates the cyberspace and internet.
- Cyber Jurisprudence deals with the composite idea of cyber jurisdiction and cyber court's venue in the cyberspace.

Jurisprudence and law

- The term Jurisprudence is derived from Latin word 'Jurisprudentia' which means either "Knowledge of Law" or "Skill of law".
- The word "juris" means law and prudentia mean knowledge, science or skill.
- Thus Jurisprudence signifies knowledge or science of law and its application.

Doctrinal approach

- Doctrinal legal research methodology, also called "black letter" methodology, focuses on the letter of the law rather than the law in action.
- Using this method, a researcher composes a descriptive and detailed analysis of legal rules found in primary sources (cases, statutes, or regulations.

Consensual approach

- The Consensual Approach thus has two initial interrelated stages: first, establishing consensus about a list of Socially Perceived Necessities (SPNs), and second showing the extent to which the people cannot afford these SPNs and are thus deprived.

Real Approach

- In practice, the caveat of cyber realists is that they use a more restrictive definition of the concepts of Security and Power.
- In theory, these concepts would not allow to include aspects related to cyber space, or other types of threat, that could affect the sovereignty of states in the international arena.

Cyber Ethics

- The term "cyber ethics" refers to a set of moral rules or a code of behaviour applied to the online environment.
- As a responsible netizen, you should observe these rules to help make cyberspace a safe place.

Jurisdictional Issues In Cyber Space

Jurisdiction in Cyber Space

- Cyberspace is a concept of recent origin and evolving everyday with the development of sophisticated technology in the form of software and hardware.
- The nature of cyberspace has challenged the traditional notion of jurisdiction of court world over.

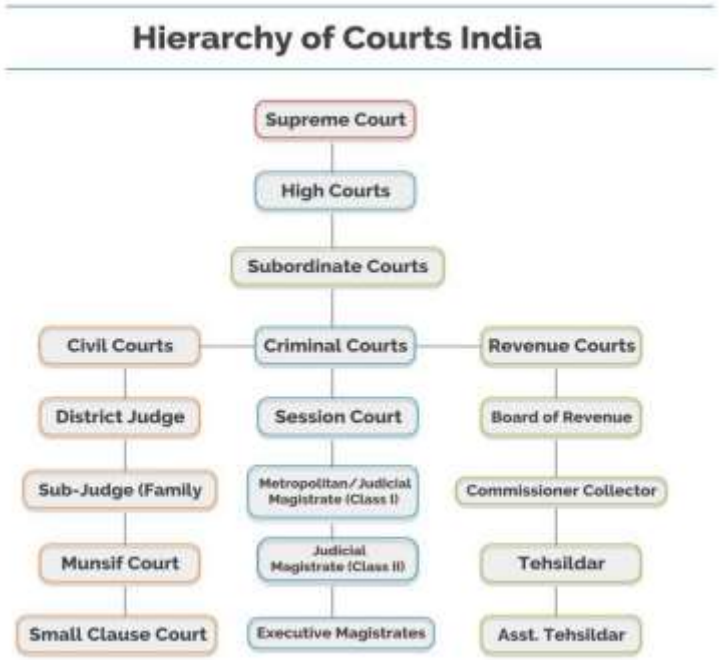
Cyber Ethics

- Some people may have a lower standard of ethics in cyberspace as they thought there is no law governing the virtual world and their anonymity will save them from being detected.
- In fact, these are all misconceptions.
- The law also governs the Internet and you may attract legal liabilities if you perform the following activities:
- posting obscene and indecent content on the Internet;
- obtaining property or services online by deception;
- spreading viruses or malicious codes; and
- Gaining unauthorised access to computers, etc.

Cyber Ethics

- Jurisdiction is the power of State to regulate the conduct of its subjects by legislations, adjudication and enforcement.
- The current module only deals with the adjudicative jurisdiction of court prescribe by State to resolve issues and fix the liability of parties.

Hierarchy of courts



Hierarchy of courts

Supreme Court

- The Supreme Court has original, appellate and advisory jurisdiction. Its exclusive original jurisdiction includes any dispute between the Centre and State(s) or between States as well as matters concerning enforcement of fundamental rights of individuals.
- The appellate jurisdiction of the Supreme Court can be invoked by a certificate granted by the High Court concerned in respect of any judgment, decree, or final order of a High Court, in both civil and criminal cases, involving substantial questions of law as to the interpretation of the Constitution or any law.
- The appellate jurisdiction of the Supreme Court can also be invoked through the residuary power of Special Leave Petition, which is to be exercised only in cases when any substantial question of law is involved, or gross injustice has been done. Supreme Court decisions are binding on all Courts/Tribunals in the country and act as precedence for lower courts.
- Under Article 141 of the Constitution, all courts in India are bound to follow the decision of the Supreme Court as the rule of law.
- Further, Article 142 of the Constitution empowers the Supreme Court to pass any order as may be necessary for doing complete justice between the parties.

Hierarchy of courts

High Courts

- High Courts have jurisdiction over the States in which they are located. There are at present, 25 High Courts in India.
- However, few of the High Courts have jurisdiction over more than one State or Union Territories: Bombay (Mumbai) High Court, Calcutta High Court (Kolkata), Guwahati High Court, High Court of Judicature at Hyderabad, Madras (Chennai) High Court and Punjab and Haryana High Courts.
- For instance, the Bombay High Court is located at Mumbai, the capital city of the State of Maharashtra. However, its jurisdiction covers the States of Maharashtra and Goa, and the Union Territories of Dadra and Nagar Haveli as well as Daman and Diu. Predominantly, High Courts can exercise only writ and appellate jurisdiction, but a few High Courts have original jurisdiction and can try suits.
- High Court decisions are binding on all the lower courts of the State over which it has jurisdiction.

Hierarchy of courts

District Courts

- District Courts in India take care of judicial matters at the District level.
- Headed by a judge, these courts are administratively and judicially controlled by the High Courts of the respective States to which the District belongs.
- The District Courts are subordinate to their respective High Courts. All appeals in civil matters from the District Courts lie to the High Court of the State.
- There are many secondary courts also at this level, which work under the District Courts.
- There is a court of the Civil Judge as well as a court of the Chief Judicial Magistrate.
- While the former takes care of the civil cases, the latter looks into criminal cases and offences.

Hierarchy of courts

Lower Courts

- In some states, there are some lower courts (below the district courts) called Munsif's courts and small causes courts.
- These courts only have original jurisdiction and can try suits up to a small amount.
- Thus, Presidency- Small Causes Courts cannot entertain a suit in which the amount claimed exceeds Rs. 2,000.
- However, in some States, civil courts have unlimited pecuniary jurisdiction.
- Judicial officers in these courts are appointed on the basis of their performance in competitive examinations held by the various States' Public Service Commissions.

Hierarchy of courts

Commercial Courts

- Commercial Courts, Commercial Appellate Divisions as well as Commercial Divisions in High Courts were constituted under Commercial Courts Act, 2015 throughout India to specifically deal with matters pertaining to “commercial disputes” of a value more than Rs.3,00,000, arising out of a wide range of transactions, including export/import, maritime, franchising, distribution & licensing, consultancy, joint venture, intellectual property, insurance, investment agreements etc.
- As specified in the Commercial Courts Act, 2015.
- The procedure followed by Commercial Courts is different and stricter in some aspects than the procedure as applicable to adjudication process of other civil disputes in general.

Hierarchy of courts

Tribunals

- Special courts or Tribunals also exist for the sake of providing effective and speedy justice (especially in administrative matters) as well as for specialized expertise relating to specific kind of disputes.
- These Tribunals have been set up in India to look into various matters of grave concern.

CIVIL AND CRIMINAL JURISDICTIONS

- Civil law handles disputes between individuals, or between an individual and another private entity, such as a company or organization. In a civil case, it is usually claimed that one party is the victim of an offense or negligence done by the opposing party and resulting in loss or damage. In such cases, civil jurisdiction can provide benefit to the injured party in the form of some type of compensation, and can also serve to hold the injurious or negligent party accountable for their actions. The following are some of the more common case types handled under civil jurisdiction:

- Personal injury
- Breach of contract
- Negligence resulting in death, injury, or other damage
- Child custody cases
- Divorce

CIVIL AND CRIMINAL JURISDICTIONS

- Definition and Examples of Criminal Jurisdiction
- Criminal law, on the other hand, is a system of legislation dealing with offenses which are deemed to be perpetrated against the government or society. Even though the victim may be an individual and not society at large, such as in a case of murder or assault, the offense may still be considered a criminal case when it involves lawbreaking action. Criminal law aims to punish people who commit crimes, rather than settle disputes between individual parties. Some examples of behaviors which would be dealt with under criminal jurisdiction include:

- Murder
- Theft or burglary
- Drunk driving
- Assault
- Domestic violence
- Illegal substance use

Cyberspace

Cyberspace and its Meaning

- The term Cyberspace seemed to have originated from a Science fiction movie.
- However, in the 21st century, it has become an integral part of our lives.
- Let us learn what Cyberspace is, the importance of laws to determine Cybersecurity in the introduction of Cyberspace.

Cyberspace

- What is Cyberspace Definition?
- The best way to define Cyberspace is the virtual and dynamic space created by the machine clones.

- According to the Cyberspace definition, it is a web consisting of consumer computers, electronics and communication networks by which the consumer is connected to the world.

Cyberspace

- **Cyberspace History**
- The word Cyberspace first made its appearance in Wiliam Gibson's Science fiction book Necromancer. The book described an online world filled with computers and associated societal elements. In that book, the author described Cyberspace as a 3D virtual landscape created by a network of computers. Although it looks like a physical space, it is generated by a computer, representing abstract data.

- After the publication of the book, the word Cyberspace became a mainstay in many English dictionaries. The New Oxford Dictionary of English provides Cyberspace definition as the notional environment used by the people to communicate over networks of the computer.

- As per the Cyberspace meaning, Cyberspace is a virtual space with no mass, gravity or boundaries. It is the interconnected space between networks of computer systems.

- Bits and Bytes- Zeroes and ones are used to define Cyberspace. It is a dynamic environment where these values change continuously. It can also be defined as the imaginary location where two parties can converse.

web hosting and web Development agreement

- Look and Feel Clause. The agreement should include a detailed, written description of both what the web site will look like and how the web site will function and perform.
- Although this sounds simplistic, many of these relationships turn sour when multiple change orders and the related increases in development costs start flying back and forth between customer and developer.
- The further you digress from this approach, the more risk you assume in higher development costs and not getting a web site that accomplishes your objectives. Any changes to the description that occur during the development process should be put in writing.

- Responsibilities Clause. The agreement should include a detailed description of each parties' responsibilities during the development process.
- The agreement should specify who will do what.
- What is left unsaid or unwritten can often cause disputes later on in the development process. The agreement should either state that the customer has no role in the development process or spell-out in detail what obligations the customer has in such regard.

web hosting and web Development agreement

- Development Schedule. The agreement should contain a detailed development schedule tied to periodic payments for interim deliverables.
- The agreement should have a start date and an end date for the developer's work. An initial payment to cover development costs is typical, but the customer should retain at least 30% of the total development cost until it is determined that the entire website is complete and conforms to the description included as part of the agreement.
- This acceptance test by the customer is a critical part of the development process.
- The further you stray from this disciplined approach, the greater risk you assume that the website will not be completed on time and within budget.

- Ownership Clause. The agreement must address the issue of who owns the finished website and its underlying work product.
- This issue raises a classic conflict between the customer's desire to preserve the uniqueness of its site and the developer's desire to recycle as much of the work product as possible for other customers. One approach is to protect the truly unique elements of the site by means such as (a) not allowing any reuse of such elements by the developer for any of its customers for a period of time or (b) prohibiting the developer from making these elements available to any competitor of the customer.

web hosting and web Development agreement

- Intellectual Property Clause. The agreement should protect the customer from unauthorized uses of intellectual property by the developer.
- The developer must warrant that it either owns or is authorized to use the tools and technology it utilizes to create the website
- . This is increasingly important if the developer is providing any kind of content for the website.
- Furthermore, the developer should be required to indemnify and hold the customer harmless from any liability arising out of a breach of this warranty.
- Exposure for this risk should be shifted entirely to the developer to the fullest extent possible.

- Developer's Post Completion Obligations. The agreement should describe any post-completion obligations of the developer.
- Provisions for on-going maintenance and support by the developer should be addressed. Similarly, the developer's obligation to provided enhancements to the site to address things like changes in browser technology should be addressed as well.

Internet as a tool for global access.

Uses of Internet:

- Internet is a very good medium to connect with the outer world. People use it as a medium to connect with other people sharing files, entertainment and lots of other activities that are useful and beneficial in many ways. The few dominant reasons why people use the Internet are given below:
-
- Information: People browse Internet for information. They love to browse various search engines like Google, Yahoo to know about any necessary news. Also they love to browse websites like Wikipedia which is a full fledged encyclopedia on Internet.
-
- Social Networking: Social networking is a good medium to communicate with friends and family members. There are many social networking sites like Face book, Twitter etc which are used by people in connecting with friends.
-
- Communication: Communication is another way to use the Internet. People connect with others through various IM services like GTalk, Skype and Yahoo messenger. There are lots of other services through which people send messages.

Internet as a tool for global access.

- Transfer of Files: People – school students, college students, office staff, businesspeople, everyone sends files through the Internet.
- This is an essential part of their lives. These files are sent through the Internet. People use various mail services like Gmail, Yahoo mail, Hotmail etc to send files.

- Current News: It is either latest news, or Sport updates; people love to surf Internet to get live update of any news. Websites like Rediff, NY times are quick news providing websites.

Legal and Technological Significance of domain Names

- Introduction

- In 2020, when the world was occupied with a ceaseless wrestle with COVID-19, numerous business visionaries accepting to the present circumstance as a chance to construct their vocation, generally by means of the internet as it is the quickest method of spreading data and having a name on the lookout.

- The development of a computer is one of the most esteemed gifts of science. The wide use of the PC provoked to the further improvement in many fields of life through the media of Internet. In the mid 1990's Internet was primarily used to send sends and accumulate data.

Legal and Technological Significance of domain Names

- Presently with the ascent of web-based business there is fast improvement in business exercises coming to pass through the net. Today, Internet energizes us in all walks around our life, from web-based banking, e-wallet, e-administration, online question goal system, data, innovation; the internet has been a platform for development and improvement in each field.

- While the advantages of using Internet are unquestionable, it isn't liberated from the adverse consequences. The internet has been leaned to different maltreatment by virtue of its inborn nature of having no restrictions. It has made the way for unmistakable kinds of infringement and different intricacies in the virtual world.

What is Internet?

- The Internet is a worldwide network of computers making use of a group of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol) that supports interconnection of a number of different computer networks.
- The Internet can be defined as the wired or wireless mode of communication through which one can receive, transmit information that can be used for single or multiple operations.

- The Internet in simple terms is a network of the interlinked computer networking worldwide, which is accessible to the general public.
- These interconnected computers work by transmitting data through a special type of packet switching which is known as the IP or the Internet protocol.

Internet as a tool for global access.

- Internet has emerged of prime importance in today's drastic shift from print to digital information and it has become the primary source of information, knowledge sharing, social networking etc which requires people to gain and equip themselves with new skills and knowledge in using the Internet for their easy and wide use.
- The Internet connects the corners of the cobwebbed world from the remotest corner to the busiest city.

Information technology Act 2000

- Important enactments of the Indian Parliament are crucial topics coming under the polity and governance segments of the UPSC syllabus.
- The Information Technology Act, 2000 (also known as the IT Act 2000 in short) is an important legislation that is frequently referred to in the daily news.
- In this article, you can read the salient features of the act and also about the controversial Section 66A of the IT Act 2000.

Information technology Act 2000

IT Act, 2000

- The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce.

- The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime.
- Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged.
- The law prescribes penalties for various cybercrimes and fraud through digital/electronic format.
- It also gives legal recognition to digital signatures.
- The IT Act also amended certain provisions of the Indian Penal Code (IPC), the Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872 and the Reserve Bank of India Act, 1934 to modify these laws to make them compliant with new digital technologies.
- In the wake of the recent Indo-China border clash, the Government of India banned various Chinese apps under the Information Technology Act. Read more about this in an RSTV titled, 'TikTok, Other Chinese Apps Banned'.

Information technology Act 2000

- The Information Technology Act, 2000 provides 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 paperbased 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 Banker’s Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention there under committed outside India by any person.

Information technology Act 2000

What is the main provision of IT Act 2000?

- The original act addressed electronic documents, e-signatures, and authentication of those records.
- It also enacted penalties for security breach offenses including damaging computer systems or committing cyber terrorism.

Amendments and Limitations of IT Act

- Amendments Brought in The Information Technology Act, 2000 The Information Technology Act, 2000 has brought amendment in four statutes vide section 9194.
- These changes have been provided in schedule 1-4.
- The first schedule contains the amendments in the Penal Code. It has widened the scope of the term “document” to bring within its ambit electronic documents. The second schedule deals with amendments to the India Evidence Act.
- It pertains to the inclusion of electronic document in the definition of evidence. The Third schedule amends the Banker’s Books Evidence Act. This amendment brings about change in the definition of “Banker’s-book”.
- It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression “Certified-copy” to include such printouts within its purview.

Amendments and Limitations of IT Act

- The fourth schedule amends the Reserve Bank of India Act.
- It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution. A major amendment was made in 2008.
- Amendment introduced the Section 66A which computer penalized sending of “offensive messages”. It also introduced the Section 69, which gave authorities the power of “interception or monitoring or decryption of any information through any resource”.
- It also introduced penalties for child porn, cyber terrorism and voyeurism. Amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.

Amendments and Limitations of IT Act

- What are the features of IT Act 2000?
- Features of the Information Technology Act, 2000

- All electronic contracts created through secure electronic channels were legally valid.
- Legal recognition for digital signatures.
- Security measures for electronic records and conjointly digital signatures are in place.

Digital Signatures

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software.
- It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.
- A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

- Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions and digital messages.
- Signers can also use them to acknowledge informed consent.
- In many countries, including the U.S., digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

Digital Signatures

- Digital signatures are based on public key cryptography, also known as asymmetric cryptography.
- Using a public key algorithm, such as Rivest-Shamir-Adleman, or RSA, two keys are generated, creating a mathematically linked pair of keys: one private and one public.

- Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys.
- For encryption and decryption, the person who creates the digital signature uses a private key to encrypt signature-related data.
- The only way to decrypt that data is with the signer's public key.

Cryptographic Algorithm

- Cryptography is a process of hiding transmitted information by the sender such that it may be read only by the intended recipient.
- In this article, we will learn more about various cryptographic algorithms.
- Cryptography is widely used in various fields such as end-to-end messaging, banking and finance, secure web communication, and access control.

Cryptographic Algorithm

- A cryptographic algorithm is a set of steps that can be used to convert plain text into cipher text.
- A cryptographic algorithm is also known as an encryption algorithm.

- A cryptographic algorithm uses an encryption key to hide the information and convert it into an unreadable format.
- Similarly, a decryption key can be used to convert it back into plain-readable text.

Public Cryptography

- Public key cryptography is a method of secure communication that uses a pair of keys, a public key, which anyone can use to encrypt messages or verify signatures, and a private key, which is kept secret and used to decrypt messages or sign documents.
- This system ensures that only the intended recipient can read an encrypted message and that a signed message truly comes from the claimed sender.
- Public key cryptography is essential for secure internet communications, allowing for confidential messaging, authentication of identities, and verification of data integrity.

Private Cryptography

- In private key cryptography, the key is used for both encryption and decryption and is shared by all parties that need to operate on the plaintext or ciphertext.
- In public key cryptography, a public and a private key are used.

Electronic Governance

- Electronic governance or e-governance implies government functioning with the application of ICT (Information and Communications Technology).
- Hence e-Governance is basically a move towards SMART governance implying: simple, moral, accountable, responsive and transparent governance.

Electronic Governance

Interactions in e-Governance:

- There are 4 kinds of interactions in e-governance, namely:
- G2C (Government to Citizens) — Interaction between the government and the citizens.
- This enables citizens to benefit from the efficient delivery of a large range of public services.
- Expands the accessibility and availability of government services and also improves the quality of services.
- The primary aim is to make the government citizen-friendly.

Electronic Governance

G2B (Government to Business):

- It enables the business community to interact with the government by using e-governance tools.
- The objective is to cut red-tapism which will save time and reduce operational costs.
- This will also create a more transparent business environment when dealing with the government.
- The G2B initiatives help in services such as licensing, procurement, permits and revenue collection.

Legal Recognition Of 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.

Electronic Governance

- G2G (Government to Government)
- Enables seamless interaction between various government entities.
- This kind of interaction can be between various departments and agencies within government or between two governments like the union and state governments or between state governments.
- The primary aim is to increase efficiency, performance and output.

Legal Recognition of Digital Signature

- This article deals primarily with digital signature (DS) and the law connected therewith.
- At the outset it is to be made clear that all the aspects of the law and all the provisions contained in various enactments related to digital signature are not dealt with in this article.
- Therefore the discussion is not in any way exhaustive.

- We are very much familiar with the signature we put with the help of our hand using pen/pencil or other writing materials.
- We also sometimes get our signature embossed on a rubber or metallic stamp and affix it especially when a large number of signatures is to be affixed.
- We use different techniques while selecting our signature. Some simply write their names while others use a different style in the writing of their names.
- We also find that some people use totally unidentifiable marks or symbols and we cannot trace out their names from their signatures.

Legal Recognition of Digital Signature

- The word sign™ is defined under Section 3(56) of the General Clauses Act 1897 as follows. Sign™ with its grammatical variations and cognate expressions, shall, with reference to a person who is unable to write his name, include mark™, with its grammatical variation and cognate expressions.
- Thus the General Clauses Act 1897 did not actually define the term but only states that it would include even a mark™ in the case of persons unable to write their names.
- In the Webster's New World Dictionary, the word sign™ means to write one's name on, as in acknowledging authorship, authorizing action etc.

Legal Recognition of Digital Signature

- The word signature™ is therefore to be construed according to the meaning of the word sign™ as discussed in the above paragraph.
- A signature is the writing or otherwise affixing a person's name or a mark to represent his name by himself or his authority with the intention of authenticating a document as being that of, or as binding on, the person whose name or mark is so written or affixed.
- Putting initials is also good and equally valid as that of a signature. It may also be noted that the signature includes an impression with a rubber stamp also.

Certifying Authorities

- A certificate authority is a company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates.

Certifying Authorities

A digital certificate provides:

Authentication, by serving as a credential to validate the identity of the entity that it is issued to.

Encryption, for secure communication over insecure networks such as the internet.

Integrity of documents signed with the certificate so that they cannot be altered by a third party in transit.

These certificates allow secure, encrypted communication between two parties through public key cryptography.

The CA verifies the certificate applicant's identity and issues a certificate containing their public key.

. The CA will then digitally sign the issued certificate with their own private key which establishes trust in the certificate's validity.

Cyber Crime and Offences

- The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection.

- In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

- The law defines the offenses in a detailed manner along with the penalties for each category of offence.

- Offences
- Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber Crime and Offences

- Cyber-crime usually includes the following −

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

Network Service Providers Liability

- A business entity that provides or sells services such as network access and bandwidth by allowing access into its backbone infrastructure or access to its network access points (NAP), which consequently also means access to the Internet.
- Network service providers are very similar to or can even be considered the same as Internet service providers (ISPs), but in most cases they are the ones providing backbone services to the ISPs.

Network Service Providers Liability

- Information Technology Act, 2000
- Section 79 gives conditional immunity to (ISP) network service providers.
- It provides that a network service provider shall not be liable for any third party provider information or data made available by him if he proves that –

- The data provided by third parties has transmitted through an ISP's servers or temporarily stored or hosted.
- The offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Cyber Regulations Appellate Tribunal

- The Cyber Appellate Tribunal (CAT) stands as a critical institution in the legal landscape. .
- Established under the Information Technology Act of 2000, the CAT serves as a specialized forum for settling cyber-related disputes, ensuring that citizens have access to fair and impartial proceedings.

Cyber Regulations Appellate Tribunal

Establishment of Cyber Appellate Tribunal

- The establishment of the Cyber Appellate Tribunal (CAT) was an important moment in India's legal landscape.
- It was introduced under Section 48 of the Information Technology (Amendment) Act of 2006, which sought to address the unique challenges brought about by the digital age.
- This move was essential because, as the internet grew, so did the risks associated with it.

Cyber Regulations Appellate Tribunal

- In section 48, there are the following sub-sections:

- The central government shall, by notification, establish one or more appellate tribunals to be known as the cyber appellate tribunal.
- The central government shall also specify, in the notification referred to in subsection (1), the matters and places in relation to which the cyber appellate tribunal may exercise jurisdiction.

Cyber Regulations Appellate Tribunal

- According to sub-section 1, the central government has the power to create one or more cyber appellate tribunals (CATs), depending on the need.
- The central government also has the power to specify the matters and places in relation to which the CAT may exercise jurisdiction.
- However, according to Rule 13 of the Cyber Regulation Tribunal Rules, 2000, there will be only one cyber appellate tribunal (CAT), and its primary location for hearings is typically in New Delhi.

Cyber Regulations Appellate Tribunal

- It is important to note that Rule 13 is a subordinate law made under the authority granted by the Information Technology Act, of 2000.
- This means that the central government has the power to modify or cancel Rule 13 if necessary.

- In the second sub-section, it is stated that the government will also mention the specific subjects and locations where the Cyber Appellate Tribunal can make decisions.

Penalties and Adjudication

- The Central Government may appoint any of its officers, not below the rank of Registrar, as adjudicating officers for adjudging penalty under the provisions of the Act.

- Before adjudging penalty, the adjudicating officer shall issue a written notice in the specified manner, to the company, the officer who is in default or any other person, as the case may be, to show cause, within such period as may be specified in the notice (not being less than fifteen days and more than thirty days from the date of service thereon), why the penalty should not be imposed on it or him.

- Every notice issued under sub-rule (2). shall clearly indicate the nature of non -compliance or default under the Act alleged to have been committed or made by such company officer in default, or any, other person, as the case may be and also draw attention to the relevant penal provisions of the Act and the maximum penalty which can be imposed on the company, and each of the officers in default, or the other person.

Penalties and Adjudication

- Provided that the adjudicating officer may, for reasons to be recorded in writing, extend the period referred to above by a further period not exceeding fifteen days, if the company or officer in default or any person as the case may be, satisfies the adjudicating officer that it or he has sufficient cause for not responding to the notice within the stipulated period or the adjudicating officer has reason to believe that the company or the officer or the person has received a shorter notice and did not have reasonable time to give reply.

- If, after considering the reply submitted by such company, its officer. or any other person, as the case may be, the adjudicating officer is of the opinion that physical appearance is required, he shall issue a notice, within a period of ten working days from the date of receipt of reply fixing a date for the appearance of such company, through its authorised representative, or officer of such company, or any other person, whether personally or through his authorised representative:

Patent Law

- Patent Law Amendment Act 2005
- Salient features of the Patents (Amendment) Act 2005 related to product patents:

- Extension of product patent protection to products in sectors of drugs, foods and chemical.
- Term for protection of product patent shall be for 20 years.
- Introduction of a provision for enabling grant of compulsory license for export of medicines to countries which have insufficient or no manufacturing capacity; provided such importing country has either granted a compulsory license for import or by notification or otherwise allowed importation of the patented pharmaceutical products from India (in accordance with the Doha Declaration on TRIPS and Public Health)
- Section 3 (d) regarding patentability.

Patent Law

- Due to the new patent regime, increased prices of products was considered to be a major hindrance during the time.
- However, the government has taken proactive measures to ensure low prices for essential drugs, and has used compulsory licensing as a tool to keep exorbitant prices under check.
- The amendment intended to make Indian drug and pharmaceutical industries competitive at par with multinational companies.
- Despite initial reservations, Indian pharmaceutical companies manufacturing generic drugs have flourished in the last decade.
- Also, MNCs have opened Research and Development Centres in India.

Trademark Law

- Trademarks make it easier for consumers to quickly identify the source of a given good.
- Instead of reading the fine print on a can of cola, consumers can look for the Coca-Cola trademark.
- Instead of asking a store clerk who made a certain athletic shoe, consumers can look for particular identifying symbols, such as a swoosh or a unique pattern of stripes.
- By making goods easier to identify, trademarks also give manufacturers an incentive to invest in the quality of their goods.
- After all, if a consumer tries a can of Coca-Cola and finds the quality lacking, it will be easy for the consumer to avoid Coca-Cola in the future and instead buy another brand.
- Trademark law furthers these goals by regulating the proper use of trademarks.

Trademark Law

- Trademark rights can also be lost through improper licensing or assignment. Where the use of a trademark is licensed (for example, to a franchisee) without adequate quality control or supervision by the trademark owner, that trademark will be canceled.
- Similarly, where the rights to a trademark are assigned to another party in gross, without the corresponding sale of any assets, the trademark will be canceled.
- The rationale for these rules is that, under these situations, the trademark no longer serves its purpose of identifying the goods of a particular provider.

Trademark Law

In order to serve as a trademark, a mark must be distinctive -- that is, it must be capable of identifying the source of a particular good.

In determining whether a mark is distinctive, the courts group marks into four categories, based on the relationship between the mark and the underlying product: (1) arbitrary or fanciful, (2) suggestive, (3) descriptive, or (4) generic.

Because the marks in each of these categories vary with respect to their distinctiveness, the requirements for, and degree of, legal protection afforded a particular trademark will depend upon which category it falls within.

An arbitrary or fanciful mark is a mark that bears no logical relationship to the underlying product. For example, the words "Exxon," "Kodak," and "Apple" bear no inherent relationship to their underlying products (respectively, gasoline, cameras, or computers). Similarly, the Nike "swoosh" bears no inherent relationship to athletic shoes. Arbitrary or fanciful marks are inherently distinctive -- i.e. capable of identifying an underlying product -- and are given a high degree of protection.

Copyright Software

- Software copyright is the legal way to protect software code, which is meant to be read by machines.
- This protection helps software developers and owners prevent others from copying or using their work without permission.
- When considering how to protect software, it’s important to understand whether it is copyrighted or trademarked.

Copyright Software

- Copyright law focuses on protecting intellectual property where the idea itself is the product, such as the text in a book rather than the physical book.
- A patent protects an idea that must be made into a physical product to have value, while a trademark protects symbols or names that represent a brand but are not the product itself.

Copyright Software

- Software, being a relatively new concept, didn't initially fit neatly into any of these categories. Initially, U.S. law treated software source code like blueprints.
- However, by 1974, this view began to change. After a commission reevaluated this stance and further definitions and court cases in the 1980s, software was eventually recognized as a literary work under copyright law.
- This decision clarified that software can indeed be copyrighted, providing a clear legal framework for its protection

Copyright Software

Understanding Software Copyrights

- The main goal of software copyright is to prevent unauthorized copying, distribution, and modification of software.
- It gives software developers and companies the exclusive right to reproduce, distribute, and display their work, allowing them to earn revenue and reinvest in further development.

Copyright Software

- In many jurisdictions, including the United States, copyright is automatic upon creation and fixation in a tangible medium of expression.
- This means that as soon as software is written and saved in some form, it is protected by copyright without the need for registration. However, registering a copyright can provide additional legal benefits, including the ability to sue for statutory damages.

Copyright or Patented

- 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.

Domain Names and Copyright disputes

- A domain name dispute is a legal complaint made on the grounds that a domain name (a proprietary string of language that is registered and recognized by the Domain Name System) has been inappropriately and illegitimately used or assigned.

Domain Names and Copyright disputes

- A Domain Name is a word or a combination of words which help identify a website's association with another individual.
- Domain names are used to locate a website and are popularly known as Uniform Resource Locator (URL).
- The Internet Domain Name is very important for every business that wants to establish their name globally.
- Domain Names consist of two parts, top-level and second-level domain names.
- These are easily identifiable, for e.g. www.google.com, here 'com' is the top-level domain and 'google' is the second-level domain.
- Any individual can purchase a Domain Name from a certified Registrar for a limited amount of time which can be renewed by the registrant upon its expiry.

Domain Names and Copyright disputes

- Domain Names can be registered and protected as trademarks as long as it meets the requirements of a trademark under the Trade Marks Act 1999.
- Domain Names that are registered trademarks are universally protected primarily by the Internet Corporation for Assigned Names and Numbers (ICANN). Resultantly, in case of any abusive registrations or infringement of existing rights, an individual has the option to file a Domain Name Dispute complaint under the Uniform Domain Name Dispute Resolution Policy (at the international level) or under the .
- In Domain Name Dispute Resolution Policy (at the national level).

Domain Names and Copyright disputes

- A Domain Name Dispute may arise when there is infringing, conflicting and/or unauthorised use of a domain name on part of an individual.
- In order to successfully establish a Domain Name Dispute, the Complainant is required to satisfy the criteria laid down in the various dispute resolution policies.
- These grounds are elaborated later upon in this article.

Domain Names and Copyright disputes

- As the internet is not restricted by any borders or boundaries, and due to the global presence of most businesses, a Domain Name infringement can occur in a country different from where it is registered.
- In the event of such a trans-border infringement, the person can use the Uniform Domain Name Dispute Resolution Policy (UDRP), a standard and uniform Policy across the world, unlike domestic laws that can vary across jurisdictions.

Electronic Data Base and its Protection

- An Electronic Database is a computer-based collection or listing of information. It can include professional, peer-reviewed journal articles that are organized in a systematic way with searchable elements or fields. This allows the search to be fast and easy.

Electronic Data Base and its Protection

- Network security. Firewalls serve as the first line of defense in DiD database security. ...
- Access management. ...
- Threat protection. ...
- Information protection. ...
- Database hardening. ...
- Comprehensive data encryption. ...
- Advanced threat protection. ...
- Separate authentication accounts.

IT Act and Civil Procedure Code

- THE CODE OF CIVIL PROCEDURE (AMENDMENT) ACT, 2002 ACT NO. 22 OF 2002 [23rd May, 2002.] An Act further to amend the Code of Civil Procedure, 1908 and to provide for matters connected therewith or incidental thereto. BE it enacted by Parliament in the Fifty-third Year of the Republic of India as follows:- 1. Short title and commencement. 1. Short title and commencement.-(1) This Act may be called the Code of Civil Procedure (Amendment) Act, 2002. (2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint, and different dates may be appointed for different provisions of this Act and for different States or for different parts thereof. 2. Amendment of section 39. 2. Amendment of section 39.-In section 39 of the Code of Civil Procedure, 1908 (5 of 1908) (hereinafter referred to as the principal Act), after sub-section (3), the following sub-section shall be inserted, namely:- "(4) Nothing in this section shall be deemed to authorise the Court which passed a decree to execute such decree against any person or property outside the local limits of its jurisdiction.". 3. Amendment of section 64. 3. Amendment of section 64.-Section 64 of the principal Act shall be renumbered as sub-section (1) of that section and after sub-section (1) as so renumbered, the following sub-section shall be inserted, namely:- "(2) Nothing in this section shall apply to any private transfer or delivery of the property attached or of any interest therein, made in pursuance of any contract for such transfer or delivery entered into and registered before the attachment.

IT Act and Civil Procedure Code

- Short title and commencement — (1) This Act may be called the Code of Civil Procedure (Amendment) Act, 1999. (2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint, and different dates may be appointed for different provisions of this Act and for different States or for different parts thereof. CHAPTER II - Amendment of Sections 2. Amendment of section 26 — In the Code of Civil Procedure, 1908 (5 of 1908) (hereinafter referred to as the principal Act), existing section 26 shall be re-numbered as sub-section (1), and after sub-section (1) as so renumbered, the following sub-section shall be inserted, namely: — "(2) In every plaint, facts shall be proved by affidavit." 3. Amendment of section 27 — In section 27 of the principal Act, the following words shall be inserted at the end, namely: — "on such day not beyond thirty days from date of the institution of the suit". 4. Amendment of section 32 — In section 32 of the principal Act, in clause (c) for the words "not exceeding five hundred rupees" the words "not exceeding five thousand rupees" shall be substituted. 5. Amendment of section 58 — In section 58 of the principal Act, — (i) in sub-section (1),— (a) in clause (a), for the words "one thousand rupees", the words "five thousand rupees" shall be substituted;

IT Act
and Criminal Procedural Code

The administration of India was taken over after the rebellion of 1857 by the British crown and subsequently, the Criminal Procedure Code was enacted in the year 1861.

The enactment of 1861 made the European natives immune from the jurisdiction of the criminal courts except for the high Court.

The code was amended in the years 1872, 1882 and 1898 to ensure uniform application over British and Indian subjects.

The legacy of British India continued until the present Code came into effect in the year 1973.

IT Act
and Criminal Procedural Code

- According to Section 2(h) of the Code, an investigation is a process of collecting evidence by either a police officer or any other person that is authorised by a Magistrate to do so.

- For the purposes of investigation, cases under CrPC have been divided into cognizable and non-cognizable cases.
- Cognizable cases are serious criminal matters where the police can arrest without any warrant and can start investigating without permission by a magistrate. These cases include among others Murder, Rape, etc.
- Non-cognizable cases, on the other hand, are less serious matters where the police cannot arrest without a valid warrant and also can start the investigation only when they obtain permission from a magistrate, for instance, cases like Assault and Defamation.
- The process of investigation starts by taking cognizance of a case and is completed when the police report is submitted under Section 173.
- The process of investigation is thorough and full of intricate procedures, any irregularities in the procedure may result in the acquittal of the accused.

Relevant Sections of Indian Evidence Act

Section 3 – Interpretation Clause.
Section 4 – May Presume.
Section 5 – Evidence may be given of facts in issue and relevant facts.
Section 6 – Relevancy of facts forming part of same transaction.
Section 7 – Facts which are occasion, cause or effect of facts in issue.
Section 8 – Motive preparation and previous or subsequent conduct.
Section 9 – Facts necessary to explain or introduce relevant facts.
Section 10 – Things said or done by conspirator in reference to common design.
Section 11 – When Facts not otherwise relevant become relevant.
Section 14 – Facts showing existence of state of mind or of body or bodily feeling.

Section 15 – Facts bearing on question whether act was accidental or intentional.
Section 17 – Admission defined.
Section 21 – Proof of admission against persons making them, and by or on their behalf.
Section 22A – When oral admissions as to contents of electronic records are relevant.
Section 24 – Confession by inducement, threat or promise when irrelevant in criminal proceeding.
Section 25 – Confession to police officer not to be proved.
Section 26 – Confession by accused while in custody of police not to be proved against him.

Relevant Sections of Bankers Book Evidence Act

- Importance of this Act
- the Bankers' Books Evidence Act 1891 provides guidelines to banking institutions about legal proceedings relating to banking records. This is an Act which was brought into force to amend the Law of Evidence with respect to banking records. In every bank, bookkeeping or recording of transactions is recorded in bank books such as ledger books, registers, account books, and other books used in ordinary courses of business. If there is any discrepancy of these banking records, it will amount to a violation under this Act. Any banking institution or any company that carries out a banking function is bound by this Act if any legal proceeding is initiated against them.

Relevant Sections of Bankers Book Evidence Act

Section 2

- Section 2A It provides that certain certificates shall be accompanied with the printout or copy of printout referred in Section 2(8). They are:

- Certificate by the principal accountant of the branch manager stating that it is:
- A printout of the entry or
- A copy of such printout
- Certificate by a person in charge of the computer system containing a brief description of the computer system along with the following:
- Particulars of safeguards adopted by the system to ensure that only authorised persons have entered the data or performed any other information.
- Particulars of safeguards adopted to ensure prevention and detection of an unauthorised change of data.
- Particulars of safeguards available to retrieve lost data due to reasons such as systematic failure.

Relevant Sections of Bankers Book Evidence Act

Section 3

- Section 3 states the power of the State Government to extend the provisions of this Act. The State Government can extend the provisions of this Act to be applied to the books of any partnership or individual carrying on the business of the banker within territories that fall under its administration.
- The State government can do so by notification in the official gazette and it can also rescind such notification.

Relevant Sections of Bankers Book Evidence Act

Section 4

- Section 4 specifies certain matters which require the production of original entry for proper investigation.
- According to this section, a certified copy of an entry in a bankers' book shall be a prima facie evidence of the existence of such entry.
- The certified copy shall be admitted as evidence of matters, transactions and accounts recorded in every case.
- The certified copy shall be admissible to the same extent as an original copy is admissible.

Relevant Sections of Bankers Book Evidence Act

Section 5

- Section 5 states that in legal proceedings to which the bank is not a party, unless the court or judge makes an order for a special cause, the officer of the bank should not be compelled to either produce bankers' books for proving any content or appear as a witness for proving matters, transactions, and accounts recorded.

Relevant Sections of Bankers Book Evidence Act

Section 6

- Section 6(1) provides the provision of inspection of books by the order of the court or the judge. The court or judge may order:

- A party to a legal proceeding to be at liberty to inspect and take copies of entries in a bankers' book for purposes of such proceeding or
- The bank to prepare and produce certified copies of all such entries within a specific time accompanied by a certificate dated and prescribed in the prescribed manner, stating that no other is found in the books of the bank relating to the matter in an issue of the proceeding.

Relevant Sections of Indian Penal Code

Mob Lynching:

- It is a violent activity where a group of people on the pretext of administering justice outside the courtroom executes a presumed offender, who might be innocent as well.
- While IPC does not have any specific mention of mob lynching, it punishes the offenders of any murder under section 101(2) (punishment for murder).
- This section says: “When a group offive or more peoplecommits the murder of an assumed culprit based on factors likecaste, language, place of birth or personal belief shall be punished.
- Those who commit the crime have to face capital punishment or a prison term of seven years to life.

Relevant Sections of Indian Penal Code

False Promise to Marry:

- Under the Indian Penal Code deceitful promise to marry is criminalized. “Deceitful means” include having sex on the pretext of providing employment or promotion, inducement, or marrying after suppressing the identity.

- Clause 69 of IPC says, “If a man promises to marry a woman, but does not actually intend to marry her, and still has consensual sex with her, this will amount to a criminal offense”.
- Sex under false promises to marry, may be punished with an imprisonment that can extend up to 10 years.
- But it will be attracted only when a man makes a false promise to a woman, with the intention of breaking it, for the purpose of sexually exploiting her with her consent.

Relevant Sections of Indian Penal Code

- Attempt to Suicide:
- Under Indian Penal Code the attempt to commit suicide is not considered a punishable offense. However, it is still considered an offense when a person has the intent of restraining a government official from performing his duty. Under section 224 of IPC, ‘Whoever attempts to commit suicidewith the intent to compel or restrain a public servantfrom discharging his official duty shall be punished with imprisonment for a term which may extend to one year or with fine or with both or with the community service. This provision ensures the prevention of self-immolations and hunger strikes during protests.

Relevant Sections of Indian Penal Code

- Gender Neutrality:
- We live in a society where we ask for women empowerment among other demands. But we are forgetting one thing, in this new society no one is safe.
- Irrespective of the gender the crimes are committed and both men and women are at risk. Therefore, our law aims to bring gender neutrality in society and safeguard the rights of both males and females.

Relevant Sections of Indian Penal Code

- Fake News:
- With free internet, there are other frees as well. And the most critical free thing we are getting these days is “Fake News”.
- Since the launch of free data from Reliance Jio we have come across many lynchings and hate against each other’s religion, caste, creed, and whatnot.
- People are often seen sharing videos with different intent which was not the actual intent of it.
- For example, a video went viral and spread like fire on the internet in which a man was seen butchering the meat of an animal and the video claimed the animal to be beef.

Relevant Sections of Indian Penal Code

Sedition:

- Sedition encompasses aiding any hate activity financially, acts of subversive activities, and inducing separatist sentiments. Section 150 of the IPC deals with sedition and mentions the punishment a person will have to face in case of committing such a crime endangering the integrity of the country.
- Section 150 of IPC says, “Whoever, purposely or knowingly, by words, either spoken or written, or by signs, or by visible representation, or by electronic communication or by use of financial means, or otherwise, excites or attempts to excite, secession or armed rebellion or subversive activities, or encourages feelings of separatist activities or endangers sovereignty or unity and integrity of India; or indulges in or commits any such act shall be punished with imprisonment for life or with imprisonment which may extend to seven years and shall also be liable to fine.”
- This provision emphasizes the gravity of acts against the state and strengthens measures to safeguard the nation’s interests.

Relevant Sections of Indian Penal Code

- Inclusivity in Unnatural Sexual Offences:
- Earlier under section 377 of IPC homosexuality and unnatural sexual activities were considered crimes. However, it is not a crime anymore after modifications done under Bharatiya Nyaya Sanhita or IPC 2.0. LGBTQ+ rights are being safeguarded by excluding punishment for unnatural sexual acts between consenting adults. Through this, our legislation reflects a more inclusive and tolerant approach to personal choices and relationships.
- However, this provision of IPC is still present to deal with unnatural sexual offenses against minors, against the consent of people involved, and bestiality.

Relevant Sections of Indian Penal Code

- Defamation:
- Under IPC, the act of defamation is a punishable offense.
- The case of defamation carries a maximum sentence of two years imprisonment, a fine, or community service under section 356 of IPC 2.0 which is an amalgamation of sections 499 and 500 of the previous model of IPC.
- This emphasizes a balanced approach to protecting the reputation of people while promoting proportionate punishment.

Relevant Sections of Indian Penal Code

- In May 2023, the Reserve Bank approved a Rs 87,416 crore dividend payout to the central government for 2022-23, nearly triple what it paid in the previous year.

- Details:

- The decision was taken at the 602nd meeting of the Central Board of Directors of the Reserve Bank of India held under the chairmanship of Governor Shaktikanta Das.
- The board approved the transfer of Rs 87,416 crore as surplus to the central government for the accounting year 2022-23.
- This is a 188% jump from the last year's (2021-22) surplus transfer of Rs 30,307 crore.
- It decided to keep the Contingency Risk Buffer (CRB) at 6 per cent.
- The contingency risk buffer is a specific provision fund kept by the central bank primarily to be used during any unexpected and unforeseen contingencies.
- The Bimal Jalan Committee recommended that the CRB needs to be maintained at a range of 5.5% to 6.5% of the RBI's balance sheet.
- The board also reviewed the global and domestic economic situation and associated challenges, including the impact of current global geopolitical developments.
- The dividend could bring in additional revenue of around 0.2 per cent of GDP.

Law Relating To Employees And Internet

- Business owners must let their employees access the internet during work hours. Internet use is vital, but employers must control internet activity in and out of their company computers.
- Your business could be liable for employee misuse.

Law Relating To Employees And Internet

- Which law is related to internet?
- 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.

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.

Alternative Dispute Resolution

- The objectives of ADR include reducing the time and expense of resolving disputes 1, protecting cyber victims and improving law enforcement in cyber cases 2, preventing and efficiently resolving disputes in construction projects.

Online Dispute Resolution(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.

Online Dispute Resolution(ODR)

- 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.

Evolution and development in E_x0002_-commerce

- What Is eCommerce?
- eCommerce is a form of business performed online or over the internet. In other words, when you buy or sell something online or via an electronic medium, it is referred to as electronic commerce, popularly known as eCommerce.

Evolution and development in E_x0002_commerce

- Because of its vast reach and popularity, it has completely changed how entrepreneurs do business and has been adopted by everyone, from small businesses to big giants. But, have you ever thought about how eCommerce started and evolved over the years?

- Here's a clue- It's on a rising spree!

- These predictions about eCommerce will throw some light on its exponential growth since its inception.

- By this year-end, eCommerce sales all around the world will exceed $650 billion
- Buyers spend close to 36% of their budget on online shopping

Evolution and development in E_x0002_commerce

- When Was Online Shopping Invented?
- Online shopping was pioneered in 1979 by entrepreneur Michael Aldrich in the United Kingdom. Aldrich was able to connect a modified domestic television to a real-time multi-user transaction processing computer via a telephone line. This was in the market in 1980 and was sold as business-to-business systems purchased by prospective customers in the UK, Ireland and Spain.

- An online bookstore was one of the earliest consumer shopping experiences created by Charles M. Stack in 1992. This online store was founded three years before Amazon was founded in 1994.

Evolution and development in E-commerce

- When Was The First Online Transaction?
- New York Times issue on August 12, 1994, mentioned that the Internet Is Open and chronicled the sale between two friends of a Sting CD. The Times said, “The team of young cyberspace entrepreneurs celebrated the first retail transaction on the Internet using a readily available version of powerful data encryption software designed to guarantee privacy.”

Evolution and development in E-commerce

Here Is The Timeline Of The History Of eCommerce & Its Evolution

1960-1968- Invention & The Early Days

The development of the Electronic Data Interchange (EDI) in the 1960s paved the way for electronic commerce. EDI revolutionized traditional ways of sending and receiving documents and allowed a digital data transfer from one computer to another.

1969: CompuServe, the first significant eCommerce company, is established by Dr. John R. Goltz and Jeffrey Wilkins by utilizing a dial-up connection. This is the first time eCommerce was introduced.

1979: Michael Aldrich invented electronic shopping (he is also considered as founder or inventor of eCommerce). This was done by connecting a transaction-processing computer with a modified TV through a telephone connection. This was done for the transmission of secure data.

1982: The continued growth of technology, particularly in electronics, led to the launch of the first eCommerce platforms by Boston Computer Exchange.

Evolution and development in E-commerce

- 1992: The 90s took the online business to the next level by introducing Book Stacks Unlimited as an online bookstore by Charles M. Stack. It was one of the first online shopping sites created at that time.

- 1994: Web browser tool introduced by Netscape Navigator by Marc Andreessen and Jim Clark. It was used on the Windows platform.

- 1995: The year marked the iconic development in the history of eCommerce as Amazon and eBay were launched. Amazon was started by Jeff Bezos, while Pierre Omidyar launched eBay.

- 1998: PayPal launched the first eCommerce payment system as a tool to make money transfers.

- 1999: Alibaba started its online shopping platform in 1999 with more than $25 million as capital. Gradually it turned out to be an eCommerce giant.

- 2000: Google launched the first online advertising tool, Google AdWords, to help retailers utilize the pay-per-click (PPC) context.

Evolution and development in E-commerce

- 2005: Amazon Prime membership was launched by Amazon to help customers get free two-day shipping at an annual fee.
- Etsy was launched in 2005 to enable small and medium-scale retailers to sell goods online.
- 2005: Square, Inc., as an app-based service, is launched.
- 2005: Eddie Machaalani and Mitchell Harper launched BigCommerce as an online storefront platform.
- The years experienced massive development in the sphere of eCommerce, such as:
- 2011: Google launches its online wallet payment app.
- 2011: One of the earliest moves by Facebook to launch sponsored stories for advertisements.
- 2014: Apple launched Apple Pay, an online payment application.

Evolution and development in E-commerce

- 2017 to 2024
- Significant reforms that have taken place in the eCommerce industry between these years are-

- Large retailers are pushed to sell online.
- Small businesses have seen a rise, with local sellers now operating from social media platforms.
- Operational costs have lowered in the B2B sector.
- Parcel delivery costs have seen a significant increase with the growing eCommerce industry.
- Several eCommerce marketplaces have emerged, enabling more sellers to sell online.
- Logistics has evolved with the introduction of automation tools and artificial intelligence.
- Social media has become a tool to increase sales and market brands. Sellers also use social media to sell via channels like Facebook and Instagram.
- The buying habits of customers have significantly changed.
- The COVID-19 pandemic has impacted purchase decisions, and most users are moving to eCommerce for their purchases.
- Sellers are adopting an omnichannel selling approach where they want to provide users with a consistent shopping experience across different media and channels.

paper vs paper less contracts

- An electronic contract is a legally binding agreement you can create and sign digitally rather than on paper.
- This type of contract typically leverages electronic signature software, which allows users to sign documents online, eliminating the need for physical signatures.

E-Commercemodels-B2B,B2C

B2B ecommerce utilises online platforms to sell products or services to other businesses.

B2C e-commerce targets personal consumers. A company that sells office furniture, software, or paper to other businesses would be an example of a B2B company. B2B ecommerce tends to be more complex than B2C ecommerce.

E-Commercemodels-B2B,B2C

- There are four types of B2B markets in the e-commerce industry which are Business to Consumer(B2C), Business to Business (B2B), Consumer to Consumer (C2C), Consumer to Business (C2B).
- B2B businesses are initiated by businesses and targeted to businesses. It's where businesses sell products or services to other businesses like wholesalers and retailers.
- B2C businesses being the most common, deal with businesses selling to consumers like Netflix which sells services to consumers.
- C2C is where a shopper can post a product or service to another shopper. eBay and Facebook marketplace makes it possible for C2C businesses.
- A site like Amazon is both a B2B and B2C business.

E-
security

What is the e-security?

- Electronic security systems use computer software and electronic devices to carry out a host of security functions to enhance the protection of a designated area. These systems monitor and collect data from subsystems, enabling system operators to interpret the data, determine a response, and counter events quickly.

Business taxation

- It is a mandatory financial charge imposed by the government on an organisation or an individual.
- This process of collecting business tax helps the government to develop facilities and infrastructure in the long term.

electronic payments

- An electronic payment refers to any financial transaction conducted electronically, where funds are transferred from one party to another using electronic means such as credit or debit cards, online payment systems, or mobile payments. Digital payments are usually broader in scope, including mobile and payment apps.

supply chain

- A supply chain transforms raw materials and components into a finished product that's delivered to a customer.
- It is made up of a complex network of organizations and activities, such as raw materials suppliers, manufacturers, distributors, retailers and the customer.

EDI,E-_x0002_markets

- What is EDI and e market?
- The importance of electronic data interchange (EDI) in eCommerce lies in its ability to automate and streamline the exchange of business documents between trading partners.
- By using a standardized electronic format, EDI can reduce errors, improve communication, and increase efficiency in supply chain processes.

Emerging Trends

- Legal Issues Faced By E-Commerce Businesses
- Introduction. With the advanced and increased use of online media, online business is becoming a fast emerging trend. ...
- Incorporation Problem. ...
- Trademark Security Problem. ...
- Copyright Protection Issue. ...
- Transaction Issues. ...
- Privacy Issues. ...
- Conclusion.

Emerging Trends

- Technological Innovations: Embracing AI and Augmented Reality.
- Augmented reality is the future of ecommerce technology enabling consumers to visualize products in their real-world environment before purchasing, reducing uncertainty, and increasing confidence in purchasing choices.

Case Study On Cyber Crimes

- Harassment Via E-Mails:
- Pune Citibank MphasiS Call Center Fraud
- Some ex-employees of BPO arm of MPhasiS Ltd MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber crime cases that raised concerns of many kinds including the role of "Data Protection".
- The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".
- ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in ITA-2000.
- Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

Case Study On Cyber Crimes

- Email Spoofing (Online
- A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make
- It Appear That The E-Mail Comes From Somebody Other Than The True
- Sender

Case Study On Cyber Crimes

- Mumbai: Using e-mail spoofing, fraudster dupes bank of Rs 9.94 lakh.
- In a case of cyber fraud, a nationalised bank was recently duped of Rs 9.94 lakh after a man, impersonating over phone as the director of a private company that has an account with the bank, tricked its employees into transferring the amount into his account by sending an official request using a fake email id, which looked similar to the company's original email id. Experts said the modus operandi is termed as e-mail spoofing, a type of cyber attack as part of which a fraudster sends an e-mail request to their target with an ID that resembles that of an entity known to them.

- An FIR in the latest case was lodged following a complaint made by a 57-year-old bank official at the Deccan police station in Pune city on Wednesday. The official told police that on July 2, he received a call on his mobile phone from someone who said he was one of the directors of a private company that has an account with the bank. "The bank has not been able to recover the money. We have registered the FIR and a probe is on to trace the accused. We are also tracking the beneficiary bank account (for a possible lead)," said Muralidhar Karape, senior inspector of Deccan police station.

Case Study On Cyber Crimes

- Cyber Pornography:
- Cyber Pornography has become a global problem. The government has decided to ban 827 websites that possess pornographic content following the order of Uttarakhand High Court. However, the people especially the youngsters, are so addicted to cyberporn that they try different means like VPN, DNS Server Change, or downloading Opera Mini that has inbuilt VPN activation, to view cyberporn.

- Can a person be made liable for watching porn on websites that are banned? Can the service providers be made responsible for publishing pornographic content? Are the laws sufficient to regulate cyberporn?

Case Study On Cyber Crimes

- Cyber Pornography
- Cyber Pornography means the publishing, distributing or designing pornography by using cyberspace. The technology has its pros and cons and cyber pornography is the result of the advancement of technology. With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online.

Case Study On Cyber Crimes

- Obscenity and Pornography
- Obscenity and Pornography are often used synonymously. But it should be noted that obscenity is a wider concept than pornography. Obscenity means anything which is immoral and against the sentiments of people, whereas pornography refers to the act of causing sexual excitement through films, pictures or books. Thus, pornography is just a part of obscenity.

Case Study On Cyber Crimes

- Porn Content
- 30% of Internet content is porn. One can get abundant access to pornographic content on the dark web. Dark web even contains the child pornographic contents. It is worthy to note that only 10% of the total content is available on the surface web, the rest of the content is available on the dark work and the deep web.
- In the year 2005, there were more than 2 billion searches for porn.
- Almost 20% of the mobile phone searches are for porn.
- 28,258 users watch porn every second.
- 90% of boys and 60% of girls watch porn by the time they turn 18.

Case Study On Cyber Crimes

- Warning against "revenge pornography", setting limits to online friendships, valuing consent and reporting to elders if faced with a problem, are among lessons the Central Board of Secondary Education (CBSE) wants teenagers to learn to ensure their safety in the virtual world.

- While the digital exposure of students has increased due to teaching activities moving completely online during the coronavirus-induced lockdown, concerns about the potential threats have been brought to the forefront with the recent “ Bois locker room” controversy.

Case Study On Cyber Crimes

- CBSE has shared Cyber Safety handbook with schools for class 9 to 12
- The CBSE has shared a Cyber Safety handbook with schools for class 9 to 12 students. The handbook also details guidelines for students as well as parents, listing the do's and dont's and activities to understand the sensitivity of the issue.

Case Study On Cyber Crimes

- Teenagers need to understand gender relations. Boys must learn to interact with girls on equal terms and respect them and their desires as those of human beings, not simply as objects of respect or desires.

Case Study On Cyber Crimes

- Consent must be an important part of relationships.
- Pictures, videos and other material shared in confidence cannot be published on social media without the permission of the person just because the other person does not want to continue in a relationship.
- Youngsters must learn to cope with rejection as it is a part of life but not the end of the world.

THE END