IPR module 4and5

1. Mention the laws covered by the term “CyberLaws”

Cyberlaws refer to the legal rules governing activities in the digital and online world. They regulate how people use computers, networks, and the internet, forming a legal system for the "paperless world." The key areas covered under cyberlaws include:

1. **Cybercrime Laws** – dealing with offenses like hacking, identity theft, and cyberstalking.
2. **Cyber Contracts and E-Commerce Laws** – regulating digital agreements and online transactions.
3. **Intellectual Property Laws** – protecting digital content like software, music, and trademarks.
4. **Data Protection and Privacy Laws** – ensuring the secure handling of personal and sensitive data.
5. **Jurisdiction and Regulation Laws** – determining legal authority in internet-based disputes.
6. **Freedom of Expression and Content Regulation** – balancing rights with control of harmful or illegal content.

These laws are essential for maintaining safety, trust, and legality in cyberspace.

---

2. Explain the need for having explicit laws for cyberspace?

Widespread Use of Internet: Computers and the internet are essential in modern business, education, communication, and governance. For example, online banking and digital payments are now common.

No Geographical Boundaries: The internet has no territorial limits, making it difficult to apply traditional laws across borders. A cybercriminal in one country can target victims in another.

Rise in Cybercrimes: Cybercrimes such as hacking, phishing, data theft, online scams, and ransomware attacks are increasing. Example: The WannaCry ransomware attack affected systems in over 150 countries.

Protection of Intellectual Property: Digital content like software, music, and videos can be easily copied or pirated. Cyberlaws help protect copyrights and trademarks.

Regulating E-Contracts and Transactions: Online businesses rely on digital contracts and electronic signatures. Cyberlaws ensure these are legally valid.

---

3. Define Cybersquatting with examples. Outline the types of cybersquatting

Definition of Cybersquatting:
Cybersquatting refers to the practice of registering, using, or selling a domain name that is identical or confusingly similar to a registered trademark, brand, or person's name, in **bad faith**. The intention is often to profit from the reputation of others. A cybersquatter typically has no legitimate interest in the domain name and may aim to deceive or mislead users.

Examples of Cybersquatting:

- Registering **twiitter.com** (a typo of Twitter) to gain traffic from typing mistakes.
- Someone buying **madonna.com** and trying to sell it back to the celebrity at a high price.
- Setting up **facebook.shop** to sell unrelated products by misleading customers.

Types of Cybersquatting • Typosquatting • Top level domain (TLDs) Exploitation Cybersquatting • Gripe Sites Cybersquatting • Look-Alike Domain Cybersquatting • Misleading Subdomain Cybersquatting • Celebrity Name Cybersquatting • Expiration Date Exploitation Cybersquatting • Homograph Attacks

---

4. Explain how cybersquatting can be recognized ?

1. **Similarity to Trademarks or Brand Names:**
   - A domain name that is **identical** or **confusingly similar** to a registered trademark or well-known brand can be a sign of cybersquatting.
   - Example: *Googlle.com* or *Micosoft.com* (instead of Google.com or Microsoft.com).
2. **Intent to Profit from Reputation:**
   - If the domain is registered with the **intent to sell it at a premium price** to the original brand owner, this is a clear indicator of cybersquatting.
   - **Example:** A domain like *amazonxyz.com* being sold to Amazon at a high price.
3. **No Legitimate Use of Domain:**
   - If the domain name has no **real business or website content** and is only being held to **exploit the brand's reputation**, it's a sign of cybersquatting.
   - Often, these sites will be used to show **ads**, **redirect users**, or even run **malware**.

4. **Domain Registration in Bad Faith:**
    - Cybersquatting can be recognized if the domain name was registered **in bad faith**, with the intention of **misleading users**, harming a brand's reputation, or gaining financial profit through confusion or fraud.

---

7. Elaborate the iliabilities of ISPs in cyberspace?

• ISP is an entity that connects people to the Internet and provides other allied services such as

• Web site building and hosting •

Access Providing

The function of an Internet Service Provider(ISP) is to provide internet service in the form of web pages, text, audio, video etc.

• Internet users may be involved in various crime activities in the cyber world

• The liabilities of ISPs arise in areas like criminal law, Torts law, Trade secret law, Copyright law etc.

•An it is impossible to monitor the activities of users on the internet, ISPs do not have any legal liability regarding the cyber crimes committed

• The WIPO copyright Treaty states that the mere provision of physical facilities for enabling or making a communication does not by itself amount to a communication

• The liability of an ISP for his action or omission be first determined in accordance with the statute under which it arises and then if at all the ISP is held liable, his liability again be filtered through section 79 of the IT Act

chapter XII of the Act provides for issues regarding the liability of the service providers

• Section 79 of the IT ACT exempts ISP's from liability if they can prove • They had no knowledge about the infringement • However, if the ISP is notified that infringing material is being stored or passing through servers, it must take appropriate action to remove or disable that material; otherwise, it may be held liable

• Due diligence was exercised for prevention of such acts • If an ISP encounters suspicious circumstances, it may be subject to "due diligence," to further

investigate whether the material hosted or refers to is unlawful and, if so, to block access

---

6. Define Linking, Hyperlinking, Deeplinking, Framing?

🔹 1. Linking or Hyperlinking

- **Linking or hyperlinking is the process of connecting one website to another by embedding a clickable link (URL).**
- **It allows a user to access content of one site while browsing another.**
- **A hyperlink can lead to the homepage, specific pages, or deep internal pages (deep linking).**
- **If a website links to another without permission, it may result in copyright infringement, especially if the intention is to gain traffic or revenue.**
- **Example: In *Ticketmaster Corp. vs Microsoft Corp.*, Ticketmaster sued Microsoft for linking to its event pages without permission, as Microsoft was earning from advertisements.**
- **Deep linking and inline linking can raise legal issues if they bypass homepages or interfere with copyright.**

🔹 2. Framing

- **Framing is a technique where content from another website is embedded within a frame (a section) on the original site.**
- **The content appears to be part of the framing website, but it actually belongs to another site.**
- **The user may not realize they are viewing content from a different website.**
- **The browser continues to show the URL of the framing site, not the source site.**
- **This can mislead users and affect the original site's branding, advertisement revenue, or user traffic.**
- **However, unlike linking, framing is less likely to be treated as copyright infringement unless there's clear damage to the copyright holder.**
- **Framing can also lead to confusion, misrepresentation, or passing off in trademark law.**

✅ Example of Framing:

A news aggregator site displays a live weather report from the official weather site inside a frame. The user thinks they are using the aggregator's service, but the content is actually coming from the weather website. If the framing site earns ad revenue while hiding the original source, it may be challenged legally.

---

5. Elaborate the role of ISPs in cyberspace?

ISP (Internet Service Provider) is an organization that offers users access to the **internet**.

ISPs provide services like **website hosting**, **domain registration**, **email**, and **data transfer**.

They allow users to view content like **web pages, videos, images, emails**, etc.

ISPs act as a **bridge between users and the global internet** infrastructure.

They are involved in handling **network traffic**, managing **IP addresses**, and ensuring **connectivity**.

ISPs may also offer **security features** like firewalls, spam filters, and parental controls.

In cyberspace, ISPs play a key role in the **smooth functioning of online communication and business**.

However, users may use the internet for **illegal activities**, and ISPs must follow laws and regulations.

Under **Section 79 of the IT Act**, ISPs are **not liable** for users' actions if:

- They had **no knowledge** of the illegal activity.
- They take **quick action** after being notified.
- They follow **due diligence** in preventing misuse.

ISPs must **remove or disable** access to illegal content when informed.

They are **not responsible** for monitoring all internet activity but must act if issues are reported.

---

8. Identify the challenges of protecting patents in cyberspace?

Pure Software Patents Not Allowed

- In India, **pure software** cannot be patented. Even if the software is complex, it is not eligible for patent protection on its own.

Computer Programs Are Not Patentable

- **Computer programs** or software code cannot be patented in India. This applies even if the software is new or highly sophisticated.

Protection Against Reverse Engineering

- If software is part of a patented invention, others cannot **reverse-engineer** it to steal or resell it. This provides some protection, even if the software itself isn't patentable on its own.

Software Can Be Patented With Hardware

- If a **novel software** works in combination with **novel hardware**, it can be patented. The combination must provide a **functional solution** that has **practical industrial use**.

Example: Apple's Patent

- Apple got a patent for the invention **"Unlocking a Device by Performing Gestures on an Unlock Image"**. Here, **software** (gesture recognition) works with **hardware** (touchscreen) to create an innovative device unlocking method, which qualifies for a patent.

Challenges in Defining Software Patents

- There is often confusion about what counts as **software-related inventions**. Some software innovations that are just algorithms or abstract ideas don't meet the **patentability requirements** in India.

---

9. Explain how copyright can be protected in cyberspace?

• In India "copyright" means exclusive right subject to the provisions of law to do or authorize the doing of act in respect of work or any substantial part of work

• A software on the internet can be created online or offline and is transmitted online

• An internet user can use it online or offline

• All kinds of software viz. commercial software, shareware, freeware and public domain software are equally protected by copyright law

• The copyright in computer software would subsist in case the software produced is original

• The copyright Act is not concerned with the originality of ideas but is concerned with the expression of thought

• Copyright subsists in a computer program provided sufficient effort or skill has been done to give it a new and original character. A software cannot claim a copyright protection if the skill or effort used is very little

based on the avaailability ont he internet ,sw can be classified into

Commercial Software

- This software is sold for a **price**.
- A significant issue with commercial software is the prevalence of **piracy**, where unauthorized copies are distributed and used illegally.

Freeware

- Freeware refers to software that is **available for free**.
- Users are permitted to **use** the software but are **not allowed** to modify or distribute it.
- Freeware can be **downloaded** and used without charge but often comes with a license restricting how it can be used.

Shareware

- Shareware is distributed freely, but it is usually available for a **trial period** before requiring the user to **purchase** the full version.
- Users can try the software, but they are not allowed to modify or redistribute it without the author's permission.

Copylifting Software

- Copylifting software is a more **permissive** type of software where users are free to **alter**, **add to**, or **distribute** the software with or without a fee.
- Users are **allowed to make changes** to the code and distribute their modified versions of the software.

---

10. Explain the scenarios of copyright infringement on cyberspace ?

1. **Without License Usage**
   - When any person uses or copies a copyrighted work **without a license** from the copyright owner, the Registrar of Copyrights, or without following legal conditions, it is considered infringement.
2. **Violation of Exclusive Rights**
   - If a person **does anything** that only the copyright owner is allowed to do—like copying, distributing, or displaying the work—it amounts to copyright

infringement.

3. **Permitting Public Communication for Profit**
   - If a person **allows their website or platform** to be used to **communicate copyrighted work to the public** for profit without permission, it is a violation.
4. **Unauthorized Sale or Hire**
   - Making, selling, or letting out **copies of copyrighted works** (like software, songs, or videos) without permission is an act of infringement.
5. **Illegal Import or Trade Distribution**
   - Importing copyrighted materials into India or **distributing/exhibiting** them in public **for trade purposes** without the owner's permission is also infringement.

---

11. Elaborate on key aspects and provisions of IT Act 2000 ?

11. Key Aspects and Provisions of the IT Act, 2000

1. **Introduction**
   - The **Information Technology Act, 2000** (ITA-2000) was passed by the Indian Parliament and **notified on 17 October 2000**.
   - It is the **main law in India** dealing with **cybercrimes** and **e-commerce** activities.
2. **Objective**
   - The Act aims to **regulate Information Technology**, promote **e-governance**, and enable **secure online transactions** in India.
3. **Structure**
   - The Act originally had **94 sections**, divided into **13 chapters** and **4 schedules**, covering a wide range of cyber-related provisions.
4. **Jurisdiction**
   - The IT Act has **extra-territorial jurisdiction**, meaning it applies even to offenses **committed outside India**, if the affected system is in India.
5. **Based on UNCITRAL Model Law**
   - The Act was inspired by the **UNCITRAL Model Law on E-Commerce (1996)** to ensure global uniformity.
   - This model law emphasized:
     - **Identifying the author** of electronic documents.
     - **Confirming approval** of the document’s content via digital signatures.

---

12. What are the primary objectives of IT Act 2000 ?

Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce.

Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication.

Facilitate the electronic filing of documents with Government agencies and also departments.

Facilitate the electronic storage of data.

Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions.

Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

---

14. Explain the meaning of intermediaries with reference to IT Act?

An intermediary is any person or entity that receives, stores, or transmits electronic records or provides services related to such records on behalf of another person. This includes organizations like network service providers, telecom providers, internet service providers (ISPs), search engines, web-hosting services, cyber cafes, and platforms facilitating online auctions, payments, and marketplaces.

Intermediaries play a crucial role in:

- **Hosting content**
- **Facilitating communication and data exchange**
- **Storing and evaluating information**
- **Enabling internet usage and access**

Examples include social media platforms like WhatsApp, Twitter, Instagram, Facebook; e-commerce platforms like Amazon, Myntra; and other services like Google (search engine) and cloud service providers.

---

15. Explain cyber terrorism and associated threats/?

Terrorism involves violent acts intended to cause fear or harm to individuals, groups, or nations to achieve political, religious, or economic goals. **Cyber terrorism** combines terrorism with cyberspace, involving unlawful attacks or threats aimed at **computer systems**, **networks**, and **information stored on**

computers. The goal is to intimidate or coerce governments or societies for political, social, or religious reasons.

Key Characteristics of Cyber Terrorism:

- **Predefined Attacks**: Cyberterrorist attacks are generally planned, targeting specific victims like government institutions, infrastructure, or organizations.
- **Targets**: These may include political, civil, economic, military, or energy infrastructures.
- **Attractiveness**: Cyber terrorism is appealing because it is:
  - **Cost-effective**: Requires fewer resources compared to physical attacks.
  - **Anonymous**: Perpetrators can hide their identity and location.
  - **Wide Range of Targets**: Cyber attacks can affect numerous sectors (e.g., government, business, utilities).
  - **Remote Operation**: Attacks can be launched from anywhere in the world.

Legal Provisions:

Under the **IT Act (Amendment) 2008**, **cyber terrorism** is addressed with severe penalties. **Section 66F** specifies:

- If someone, with the intent to harm the unity, integrity, security, or sovereignty of India, or to create terror among the public, **accesses** a restricted **computer resource** without authorization, they are committing **cyber terrorism**.
- **Punishment**: Life imprisonment for those convicted of cyber terrorism.

associated threats

National Security Risks: Cyber attacks can harm government and military systems, putting a country's safety at risk.

Money Losses: Attacks on banks or businesses can cause big financial problems.

Interrupting Services: Cyber terrorism can shut down important services like hospitals or power supply, affecting daily life.

---

16. Describe any 3 cybercrimes in detail

Cybercrime is a broad term used to define criminal activities where computers or computer networks are either a tool, a target, or a place for criminal activity. It includes a wide range of illegal actions, such as phishing, credit card fraud,

illegal downloading, cyber terrorism, child pornography, identity theft, and more. It can also refer to traditional crimes that are facilitated by the use of computers, like fraud calls or revenge hacking.

Three Cybercrimes in Detail

1. **Phishing**:
   - **What it is**: Phishing is when criminals use deceptive emails or websites to trick people into revealing sensitive information such as passwords, credit card details, or personal identifiers.
   - **How it works**: A victim might receive a fake email that appears to be from a trusted source (e.g., a bank) and asks them to click a link to "verify" or "update" their information. The link leads to a fake website that collects the victim's credentials.
   - **Impact**: Phishing can lead to identity theft, financial losses, and unauthorized access to personal accounts, making it one of the most common and damaging cybercrimes.
2. **Hacking**:
   - **What it is**: Hacking is the unauthorized access to a computer system or network, usually to steal, manipulate, or destroy data.
   - **How it works**: Hackers use various methods, such as exploiting security vulnerabilities, malware, or social engineering, to break into systems. They might target organizations, government entities, or individuals.
   - **Impact**: Hacking can result in stolen intellectual property, financial data, or personal information, as well as the disruption of services or operations of businesses, governments, or individuals.
3. **Cyberstalking**:
   - **What it is**: Cyberstalking involves the use of the internet or other electronic means to harass, intimidate, or track someone.
   - **How it works**: Cyberstalkers might send threatening or offensive emails, post false information about the victim online, or use social media to follow and monitor their victim’s activities.
   - **Impact**: Victims of cyberstalking may experience emotional harm, fear for their safety, and even physical harm in some cases. The effects can be long-lasting and severely affect the victim's mental health.

---

17. State the offences of misinterpretation covered by IT Act 2000?

Under Section 71 of the IT Act, 2000 (ITAA 2008), misrepresentation or suppression of material facts to obtain licenses or Electronic Signature

Certificates is considered an offence. Below are the key details related to misrepresentation offences under the IT Act:

1. **Misrepresentation to Obtain Licenses or Certificates:**
   - **Offence: Any person who makes false statements or suppresses important facts from the Controller or Certifying Authority (CA) to obtain an Electronic Signature Certificate or a license is committing a criminal offence.**
   - **Punishment: If convicted, the person can face:**
     - **Imprisonment for up to 2 years, or**
     - **A fine of up to one lakh rupees, or**
     - **Both imprisonment and fine.**
2. **Non-Cognizable Offence:**
   - **The offence under Section 71 is a non-cognizable offence, which means police do not have the authority to arrest the accused without a warrant.**
3. **Bailable Offence:**
   - **This offence is also bailable under Section 77B, which means the accused can be released on bail during legal proceedings.**

13