IPR 4AND 5 continution

13. Define Abetment. What are the punishments for abetment under IT Act?

Definition of Abetment:

Abetment involves **instigating**, **conspiring**, or **aiding** another person to commit an offence. An act is said to be committed as a result of abetment when the offence happens due to such instigation, conspiracy, or aid.

Punishment for Abetment under the IT Act:

- As per **Section 84B of the Information Technology (Amendment) Act, 2008**, any person who abets or attempts to commit a cyber offence is **liable for punishment**.
- The punishment includes:
  - **Imprisonment**: Up to **one-half of the longest term** prescribed for the main offence.
  - **Fine**: As prescribed for that particular offence.
- Even **attempts to commit a cyber offence** are punishable under this section.

Thus, both abetment and attempt to commit an offence under the IT Act are treated seriously and are punishable by law.

---

18. What are protected systems? Explain the offences and punishments related to protected systems?

✅ **Definition of Protected Systems:**

- **Protected Systems refer to critical information infrastructure (CII) resources that are essential for the functioning of the nation.**
- **Under Section 70 of the Information Technology Act, 2000, the Central Government has the authority to declare any computer resource as a "Protected System" if it directly impacts:**
  - **National Security**
  - **Economy of the country**
  - **Public Health or Safety**
- **Only authorized personnel are allowed to access such systems, and any unauthorized access is treated as a serious cyber offence.**

✅ **Examples of Protected Systems:**

- **Systems used in:**
  - **Defense and Military**
  - **Banking and Financial Sector**
  - **Power Grid and Nuclear Facilities**

✅ **Offences Related to Protected Systems (Section 70):**

- **Unauthorized access to a protected system.**
- **Hacking or tampering with the operation of the protected system.**
- **Attempting to secure access without proper authorization.**
- **Disruption or denial of service (DoS) attacks targeting protected systems.**

These actions are considered criminal offences, regardless of whether the act was successful or only attempted.

✅ **Punishment for Offences:**

- **Imprisonment up to 10 years**
- **Fine (amount decided by the court depending on severity)**
- **Both imprisonment and fine**
- **The offence is cognizable and non-bailable, meaning police can arrest without a warrant, and bail is not granted easily.**
- **The severity reflects the national importance of protected systems.**

✅ **Legal Provisions (as per IT Act):**

- **Section 70(1): Central Government may declare any computer resource as a protected system.**
- **Section 70(2): Designation of an appropriate agency or individuals to access and operate such systems.**
- **Section 70(3): Punishment for unauthorized access — imprisonment up to 10 years and fine.**

✅ **Importance of Protected Systems:**

- **Ensures national security and economic stability.**
- **Prevents cyber terrorism and infrastructure sabotage.**
- **Enables controlled and lawful access to sensitive systems.**
- **Helps in risk mitigation for critical sectors.**

---

19. Define Privacy. What is meant by violation or breach of confidentiality and privacy? Explain the punishments given for the same ?

✅ Definition of Privacy:

- **Privacy is a subjective and relative concept; it varies based on individual perception.**
- **It refers to the right of individuals, groups, or institutions to determine:**
  - **How, when, and to what extent information about their personal lives or affairs is communicated to others.**

- Privacy cannot be defined absolutely as it holds different meanings for different people.

✅ Violation of the Right to Privacy in Cyberspace:

- With the rapid growth of Information Technology in India, new avenues for infringement of privacy have emerged.
- Many internet users are unaware of the potential risks involved in sharing personal data online, especially on social networking platforms.
- Lack of security awareness, legislation enforcement, and user vigilance increases the severity of privacy violations.

✅ Violation/Breach of Confidentiality and Privacy – Legal Provisions and Punishments under IT Act:

🔹 Section 66E – Punishment for Violation of Privacy:

- Covers cases where a person intentionally or knowingly captures, publishes, or transmits the image of a private area of another person without consent.
- Such actions that violate the personal privacy of the individual are punishable with:
  - Imprisonment up to 3 years, or
  - Fine up to ₹2 lakh, or
  - Both imprisonment and fine

🔹 Section 72 – Breach of Confidentiality and Privacy:

- Applies to a person who, in the course of exercising powers under the IT Act, obtains access to electronic records or information and discloses it without authorization.
- Punishment includes:
  - Imprisonment up to 2 years, or
  - Fine up to ₹1 lakh, or
  - Both
- This offence is bailable under Section 77B of the IT Amendment Act, 2008.

🔹 Section 72A – Disclosure of Information in Breach of Lawful Contract:

- Applies to any person, including intermediaries, who:
  - Gains access to personal information while providing services under a lawful contract,
  - And discloses it without consent to cause wrongful gain or loss.
- Punishment includes:
  - Imprisonment up to 3 years, or
  - Fine up to ₹5 lakh, or
  - Both

---

20. How does cyberspace impact personal privacy? Explain with examples?

✅ Introduction to Cyberspace and Privacy:

- Cyberspace is the virtual environment where communication, data exchange, and digital interactions take place over the internet.
- Personal privacy is the right of an individual to control the access, use, and sharing of their personal information.
- In cyberspace, this right is often compromised due to various factors such as data tracking, surveillance, and cybercrimes.

✅ Major Impacts on Personal Privacy in Cyberspace:

🔹 1. Data Collection and Profiling:

- Websites, social media platforms, and mobile apps collect personal and behavioral data such as location, interests, and browsing habits.
- Example: E-commerce websites like Amazon or Flipkart track browsing history to suggest products and advertise accordingly.

🔹 2. Unauthorized Sharing of Information:

- Personal data shared online may be sold to third parties or used without consent.
- Example: Many free apps share user data with advertising companies without informing the user.

🔹 3. Social Media Overexposure:

- Users voluntarily post personal content, leading to digital footprints.
- Hackers and criminals may exploit this information for identity theft or stalking.
- Example: Posting photos of passports, tickets, or live locations can make users vulnerable to fraud.

🔹 4. Cybercrimes and Data Breaches:

- Personal privacy is at risk due to hacking, phishing, ransomware, and data leaks.
- Example: Breach of Aadhaar data exposed millions of Indian citizens to identity theft.

🔹 5. Government and Corporate Surveillance:

- Monitoring and surveillance systems used by governments or companies may invade individual privacy without user knowledge.
- Example: Use of spyware or apps with camera/mic access permissions without valid

✅

- IT Act, 2000 (Amended 2008) provides legal provisions to safeguard privacy:
  - Section 66E – Punishment for violation of privacy (3 years imprisonment or ₹2 lakh fine or both).
  - Section 72 & 72A – Breach of confidentiality and disclosure of information without consent.

- However, privacy laws are still evolving and often lack strict enforcement.

✅ Examples from Real-World Scenarios:

- Cambridge Analytica scandal – User data from Facebook misused for political profiling.
- Pegasus spyware – Allegations of illegal surveillance on journalists and activists in India.
- Aadhaar leaks – Access to sensitive citizen data was sold illegally online.

✅ Preventive Measures to Protect Privacy:

- Use strong passwords and update them regularly.
- Avoid sharing sensitive information publicly on social media.
- Read privacy policies and restrict app permissions.
- Use two-factor authentication (2FA).
- Stay informed about cybersecurity threats.