

## UNIT - 1

### 1) Explain Cyber stalking (4)

- Cyber stalking is the act of using electronic communication & online platforms to intentionally & repeatedly engage in unwelcome behavior towards an individual, causing them emotional distress or fear.
- Cyber stalkers use social media, emails, instant messaging, etc as channels to interact with their victims.
- Unfortunately, the IT Act fails to take note of it. If an email is innocently worded, it is not treated as criminal intimidation, punishable under the Indian Penal Code, 1860.
- Hence cyber stalking should have been defined & made punishable under the IT Act, 2000.

(6)

Cognizable offences	Non - Cognizable offences
<ol style="list-style-type: none"> <li>1) Offences for which arrest without warrant is provided</li> <li>2) FIR is registered</li> <li>3) Police initiates investigation without permission of the court</li> <li>4) State investigates the case from the beginning &amp; fights against the accused</li> <li>5) Burden is on the prosecutor</li> <li>6) Generally more severe crimes eg. murder, robbery, etc</li> </ol>	<ol style="list-style-type: none"> <li>1) Offences for which a warrant is required for arrest</li> <li>2) FIR is not registered</li> <li>3) Investigation cannot be initiated w/o permission of the court</li> <li>4) Complainant seeks to prosecute the accused</li> <li>5) Burden is on the complainant</li> <li>6) Generally less severe crimes eg. defamation</li> </ol>

### 3) Explain hacking (10)

- Hacking is the act of breaking into computer systems.
- Hackers have been classified as code hackers, phreakers, cyber-punks & crackers.
- Code Hackers → have knowledge of the intricacies of computer systems & their operations.
- Phreakers → have deep knowledge of the internet & telecommunication systems.
- Cyber-punks → specialize in cryptography.
- Crackers → break into computer security systems.



- Ethical hacker / white hat hacker → gains access to systems with a view to fix the identified weaknesses with written permission from the owner
- Grey hat hacker → gains access to system without authority with a view to identify & reveal the system's weaknesses to the owners
- Script kiddies → unskilled person who gains access to systems with premade tools
- Hacktivists → uses hacking to send social, political, religious messages to masses

In terms of motivating factors, 4 types of hacking are prevalent

- for fun & or as a hobby by teens obsessed with the internet
- to damage the business of competitors
- to ~~for~~ commit a further offence such as fraud or misappropriation
- by internet security companies to test their clients systems & win their confidence

4) Explain the diff categories of jurisdiction of civil courts in India (6)  
Jurisdiction of civil courts in India can broadly be classified into 3 types

i) Pecuniary jurisdiction

- Pecuniary jurisdiction implies jurisdiction based on monetary limits.
- for eg, a suit valuing above Rs 5 lakhs would have to be filed in the Delhi High Court, while those upto Rs 5 lakhs would need to be filed in district courts.

ii) Subject matter

- Jurisdiction based on subject matter means that jurisdiction for certain subjects has been exclusively vested in a particular court
- for eg, a petition for winding up of a company can be filed only in the concerned high court → liquidation

iii) Territorial jurisdiction

- Territorial jurisdiction refers to a geographical area within which a court has the legal authority to exercise its power.
- for eg, a district court in Goa has territorial jurisdiction over legal matters arising only within the geographical limits of that district & not ~~else~~ elsewhere



## 5) Diff bet<sup>n</sup> click-wrap~~ed~~ & shrink-wrap~~ed~~ contracts (6)

②

### Click wrap

### Shrink wrap

1) Agreement formed by clicking an "I agree" button or similar action during online installation or downloading of application.

2) Terms & conditions are visible on the screen & must be agreed to before installation or use of software.

3) Requires the user to consent that they accept the product

4) Common in online transactions, downloads & digital transactions

1) Agreement formed by opening or breaking the seal of a physical product

2) Terms & conditions are typically visible after opening the package since they are enclosed within it.

3) Assumes the users acceptance of the product unless they return it

4) Common in physical products like CDs or DVDs

need two more points

6) What care must be taken while formulating click wrap contracts?

- User must be expressly notified of the terms & conditions in the contract
- It must be structured in such a way that the agreement can be viewed before the option to accept or reject is provided
- In case of an accidentally agreeing, the user must be provided with a two step agreement process where they must first click "I accept" & then "I confirm"
- The user must be able to exit the process at any stage.

7) Explain Section 80 of the IT Act, 2000

(1) Notwithstanding anything contained in the Code of criminal procedure, 1973 (2 of 1974), any police officer, not below the rank of deputy superintendent of police, or any other officer of the central government or a State government authorised by the central government in this behalf may enter any public place & search & arrest without a warrant any person found therein



who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

(explain this) ↑

(2) Where any person is arrested under subsection (1) by an officer other than a police officer, such officer shall, without unnecessary delay take or send the person arrested before a magistrate having jurisdiction in the case or before the officer in-charge of a police station.

- Section 80 applies only to those offences punishable under the IT act, 2000
- Cyber crimes under other laws are not applicable here
- For example, defamation through ~~can~~ email is considered an offence under the IT Act 2000, it is covered under the Indian Penal Code, 1860. Hence Section 80 would not be applicable here

3) Explain various clauses in ~~all~~ T&Cs of contracts

i) Governing law & jurisdiction clauses

- Specifies the legal system that will govern the contract & the jurisdiction where disputes will be resolved
- Example: "This agreement shall be governed by Indian laws. The Courts in Delhi only & no other court of law, shall have jurisdiction regarding any dispute pertaining to or having any connection with this agreement"

ii) Limitation of liabilities

- It defines the extent of financial liabilities of parties in case of breach or other legal issues
- Example: "In no event shall either party be liable for any consequential, indirect or incidental damages arising out of this agreement"

iii) Warranties

- Outlines the promise made by one or all parties involved regarding the quality & performance of characteristics of goods or services



- Example: "The seller warrants that the delivered goods shall be free from defects in workmanship & materials for ~~at least~~ one year from the date of delivery"

#### 4) Non Disclosure

- Obliges one party or more parties to keep certain information confidential from third parties
- Example: "Both parties agree not to disclose any confidential information obtained during the course of this agreement to any third party without the consent of the disclosing party".

#### 5) Arbitration

- Specifies the method for resolving disputes outside of the traditional court system, often through a neutral 3<sup>rd</sup> party arbitrator or an arbitration panel
- Example

#### 6) Entire Agreement:

- Clarifies that the written contract represents the complete understanding between the parties superseding any prior oral or written agreements
- Example: "This agreement constitutes the entire understanding between the parties & supersedes all prior agreements, whether oral or written"

#### 7) Restraining employees from competitive activities

- Purpose: Restricts employees from engaging in competitive activities such as working for a rival company or starting a similar business for a specified period within a well defined area.



## a) Exclusion clauses

Where several courts ~~have~~ would have jurisdiction & parties have agreed to submit their disputes to one or more of those jurisdictions & not to others, such a clause is valid.

ie. An agreement where all parties of a contract agree to submit their disputes to a particular jurisdiction which is a proper jurisdiction under the law is valid & not void.

Section 28 of the Indian Contract Act states that when one or more than one court ~~as~~ has territorial jurisdiction, it is open for the parties to agree to confine the jurisdiction to any one or more of such courts having territorial jurisdiction.

### Abuse of this clause:-

Where the parties are unequal & an exclusion clause restricts jurisdiction to a place which would cause extreme hardships to one party where it would make it ~~is~~ almost prohibitive for them (weaker party) to litigate their claims, such a clause would be oppressive & unjust.

## 10) What is defamation?

It means causing ~~of~~ injury to the reputation of a person. It is a criminal offence under the Indian Penal ~~&~~ Code which consists of the following ingredients

- Making or ~~to~~ publishing an imputation concerning any person.
- The imputation is made with the intent to cause harm to, or knowing or having reason to believe that such an imputation will cause harm to the reputation of a person.
- The imputation is made by words that are either
  - meant to be read
  - or spoken
  - or by signs
  - or by visible representations



Example :

If A writes a derogatory letter to B, it shall not amount to defamation, though it may be covered under other offences depending on the nature of the remarks stated within.

However, if A writes a letter to C containing derogatory remarks about B which damage B's reputation, it shall amount to the offence of defamation under the law.

ii) What are cyber crimes? Explain strategies

- Cyber crimes are a broad category of crimes that involve the use of digital devices or networks.
- They are efficient & have no geographical limitations.

Strategies

- Law enforcement agencies must be trained in the intricacies of technologies so as to properly & effectively conduct investigations.
- A cyber cop must be at least half an IT engineer to be a competent cyber crime investigator.
- Besides technical knowledge, cyber cops must also learn to use technical weapons & tools such as trace & trap devices to detect cyber crimes.
- Due to the tendency<sup>of cyber criminals</sup> to jump geographical borders, there must be cooperation bet<sup>n</sup> law enforcement agencies of different countries.
- Govt should fund & support R&D that facilitates education of measures to counter cyber crimes.
- Focus should be given to the use of encryption & other security technologies.
- Govt should encourage the use of security technologies & work closely with the private sector.