Unit I

CHAPTER 2

Cyber Crime and Criminal Justice : Penalties, Adjudication and Appeals Under the IT Act, 2000

Syllabus Topic : Concept of 'Cyber Crime' and the IT Act, 2000

2.1 Concept of 'Cyber Crime' and the IT Act, 2000

Q. 2.1.1 What is cyber crime? How the classification of cyber crime is done? (Ref. Sec. 2.1) **(5 Marks)**

Q. 2.1.2 Explain the term Document and Electronic record. (Ref. Sec. 2.1) **(5 Marks)**

- The definition of cybercrime is not defined in Information Technology Act, 2000 and also its expressions are not used. The IT Act, 200 only gives the definitions of certain offences and punishments for certain offences.
- If we define cyber crime narrowly, then cybercrime is defined as the crimes which are mentioned in Information Technology Act, 2000. The cybercrimes are restricted to tamper done with the computer source code, cyber pornography, hacking, email abuse, harassment, defamation, IPR theft, cyber fraud etc.
- If we define cyber crime broadly, then cybercrime is any act of commission committed on or via or with the help of internet, whether connected directly or indirectly, which is prohibited by law and for which punishment, monetary and/or corporal is provided. This definition is applied for and punishes only certain cyber offences and is not exhaustive of all the cyber crimes.
- For example, if a person is giving death threat through the internet, he is liable for offence of criminal intimidation under Section 506 of Indian penal code 1860 and no offence under the IT Act this, offence is still known as cyber crime as per the broad definition.

Classification of cyber crime

The cyber crimes are classified as :

1. Old crimes 2. New crimes

1. Old crimes

- These crimes are committed on or via the new medium of internet. for example fraud, defamation, threats, misappropriation, cheating etc. All the mentioned crimes are old but the place of operation is new and the new place is internet. Because of the high speed of the internet and the global access, it is easy, risk free and efficient to perform such crimes.
- These crimes are cheap and profitable to commit. These crimes can be called the crimes on the internet.

2. New crimes

- These crimes are created with the internet itself for example planting viruses hacking IPR theft etc. such crimes are also known as crimes of the internet.
- New crimes are used for the commission of old crime. For example to carry out the cyber frauds hacking is committed.
- Computer crimes are also classified based on the nature of the usage of the computer.
  - Computer crimes which are committed properly for example hacking in hacking computer and networks important for commission of the offence.
  - Crimes which are assisted by computer for example cyber pornography where the medium is computer.
  - The crimes where the computer is only secondary for commission for example cyber fraud.
- There are some crimes related to cyberspace which are given in the Indian penal code 1860.
- It has been observed that in many offences in IPC the definition of document is not included within its boundary 'electronic records'.

Document

- Document under IPC Section 29 denotes any matter expressed or describe upon in a substance by means of letters, figures or marks or, by more than one of those means intended to be used or it may be used as evidence of that matter.

- It is explained in IPC Section 29 that it is immaterial by what means or upon what substance the letters, figures or marks, are formed or whether the evidence is intended for or may be used in a court of justice or not.

☞ **Electronic records**

The definition of the electronic record is given in Section 2(1)(t) in The Information Technology Act, 2000 as follows :

(t) "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.

Syllabus Topic : Hacking

2.2 Hacking

Q. 2.2.1 What is hacker? What are the different types of hackers? (Ref. Sec. 2.2) **(5 Marks)**

Q. 2.2.2 Explain how IT act defines and publishes hacking. What is the punishment for hacking? (Ref. Sec. 2.2) **(5 Marks)**

- The definition of hacker is, the people whose profession or hobby of working with computer is known as hackers or they also known as crackers.
- Another definition of hacker is, a person who enjoys exploring the details of the programming system and how to stretch their capabilities as opposed two most users who prefer to learn only the minimum necessary, or one who programmes enthusiastically is also known as hacker.
- The definition which is more commonly used for hacking is breaking into computer systems.

There are following types of hackers :

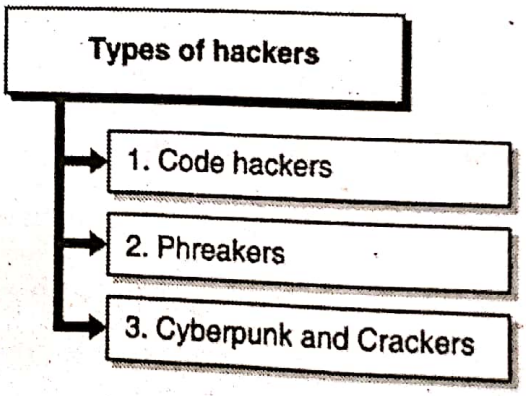

Fig. 2.2.1 : Types of hackers

➜ **1. Code hackers**

The code hackers are the people who are having the knowledge of intricacies of computer system and their operations.

➜ **2. Phreakers**

Phreakers are those people who have deep knowledge of the internet and telecommunication system.

➜ **3. Cyberpunk and crackers**

The people who are specialized in cryptography and crackers are those people who crack into computer security system.

- Criminal hacking is the biggest threat to the internet and e-commerce. Many netizens think that in internet is vulnerable and weak. If hacking is uncontrollable then it will raise question on technology so it is necessary to check for the hacking in all the circumstances if internet is used for e-commerce.
- If hacking remains unchecked and uncontrollable, then it will bring down the spirit of web entrepreneurs from entering the IT industry by putting up the websites and as a result it affects the future of e-commerce.
- E-Commerce has become costlier as there is a huge cost in world for installing systems guard against hackers. For example the Pakistani hackers have hacked Indian websites. An another example is in SEBI website link of pornographic website was inserted. Nothing is also used for doing the product again Institutions and governments.
- Hacking is done for the following purposes :
  1. Teenagers are obsessed with internet for doing hacking for fun as a hobby.
  2. The businessman does hacking to damage the business of competitor.
  3. Hacking is also done with the intention for committing fraud and misappropriation.
  4. Hacking is also done by the internet security companies for testing their clients systems and winning the confidence.
- There are many websites available on internet which tells how to crash computers and hijack control of computer systems.

☞ **The IT Act, 2000 defines and publishes hacking as follows :**

A) Section 66 Hacking with Computer System

(1) Whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing

in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.

- It is necessary to prove the following ingredients before holding a person guilty for the offence of hacking in India :
  - An act which destroys or delete or changes any information residing in a computer resource or diminishes its value of utility or affects it's ingeniously by any means.
  - The aforesaid act is committed with the intent to cause or knowing that it is likely to cause wrongful loss or damage to the public or any person.
- Like other criminal offence lease hacking needs intent or knowledge and the act of commission as given under Section 66 (1) of the IT Act, 2000.
- If hacking is done innocently or unintentionally if it causes a loss or damage to public or any person would not amount hacking.
- The internet to commit the offence or knowledge of its likely loss is the question of the fact to be gathered in fault from the circumstances of each particular case.
- **Punishment for criminal hacking** is imprisonment up to 3 years or sign up to ₹ 2 lakh or both. Victim can also claim for the damages from the hacker under civil law.
- Planting virus in computer system is also considered as hacking.
- The law of it also give gives for the damages by way of compensation not exceeding rupees one crore to the persons affected on the commission of either or more of the following acts done by any person without the permission of the owner, or any other person who is incharge of computer, computer systems, or computer networks:
  - Access to such computer, computer system or computer network. (Section 43(a) of IT Act, 2000).
  - Damage to any computer, computer system or computer network, data, computer database or any other programs residing in such computer system or computer network. (Section 43(d) of IT Act, 2000).
  - Disruption of any computer, computer system or computer network. (Section 43(e) of IT Act, 2000).
  - Assistance to any person to facilitate access to a computer, computer system or computer network in contravention of IT Act rules and regulations made there under. (Section 43(g) IT Act, 2000).

- Hacking for the purposes of it is only defined in Section 66 one of the act which has already been discussed.
- For determining the quantum of compensation Where are there or more of the four FedEx approved the adjudicating officer would be required to have safeguard to (Section 47 of the IT Act) :
  1. The amount of gain of unfair advantage, whenever quantifiable, made as a result of the default;
  2. The amount of loss caused to any person as a result of the default;
  3. The repetitive nature of the default.

Syllabus Topic : Teenage Web Vandals

2.3 Teenage Web Vandals

Q. 2.3.1 Explain teenage web vandals. (Ref. Sec. 2.3) **(5 Marks)**

- The attraction of internet has given birth to teenage cyber criminals. Now a day's cyber hacking has become attraction for the teenagers. How to hack CDS are available in the market in the cheap rate and easily.
- This CD's are having the information about hacking the internet and hijacking computer. The motivation which the teenage cyber criminals are as follows :
  1. Many teenagers are hungry for fame and publicity because of the access of the internet.
  2. Many teenagers are having excitement of achieving something great for doing something different.
  3. Some teenagers want to demonstrate their knowledge of Internet and computer programming.
  4. Many teenagers are not having the knowledge of the adverse effect of the act of hacking; they have perception that there will be no loss due to hacking.
  5. Teenager's obsession for computer programming and internet has not got the right direction.
  6. Lack of fear of law and its enforcement because of anonymity given by the various system of the internet you can say it is considered as risk free adventure.
  7. Tools required committing the hacking are cheap and getting easily.

- It is important to monitor the teenage activities on the internet to avoid the adverse effect on IT industry and on the society.
- The elder member of the family has to monitor the teen's activities.
- Parents and teachers can effectively act as policeman to prevent the teenage.

Syllabus Topic : Cyber Fraud and Cyber Cheating

2.4 Cyber Fraud and Cyber Cheating

Q. 2.4.1 Explain cyber fraud and cyber cheating. (Ref. Sec. 2.4) (5 Marks)

- From last few years so many internet frauds are increased. Maximum calls are happening in e-commerce as the e-commerce is growing rapidly.
- Many cyber frauds are not disclosed by the victim because they have the fear of losing public trust, image, confidence and business.
- Few areas where cyber frauds and cheating take place are, misusing the credit card by obtaining the password, introducing bogus investment schemes, non delivery of the goods purchases online from websites, transfer of funds etc.
- The fraud is stated in Section 17 in the Indian Contract Act, 1872 as follows : Section 17 in the Indian Contract Act, 1872.

2.4.1 Fraud

'Fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent1, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract 'fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent1, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract :

(1) The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;

(2) The active concealment of a fact by one having knowledge or belief of the fact;

(3) A promise made without any intention of performing it;

(4) Any other act fitted to deceive;

(5) Any such act or omission as the law specially declares to be fraudulent.

☞ **Explanation**

- Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak 2, or unless his silence, is, in itself, equivalent to speech.
- The expression cyber fraud is used for the purpose of criminal law; it is used for the cross under the law of contract and other civil laws. For claiming damages and compensation under the civil law, cyber fraud expression is used.
- The expression cyber cheating is used for the crime entailing corporal punishment and fine. All the frauds can be considered as cheating but it is not vice versa. Cheating offence is popularly called 420 in India cheating is defined in Indian Penal Code under Section 415 as follows :

2.4.2 Section 415 : Cheating

- Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

☞ **Explanation**

A dishonest concealment of facts is a deception within the meaning of this section.

2.4.2.1 Ingredients of Cheating

- The ingredients of cheating are as follows :
  a. The accused must have induced fraudulently or dishonestly a person.
  b. The deceived should be induced to deliver any property to any person or to consent that any person shall retain any property.
  c. If the person deceived, must be intentionally induced by the wrong-doer to do or omit to do anything which he would not do or omit if such deceived person was not so deceived.
  d. The deceived should suffer any damage or harm in body, mind, reputation or property by the deceitful act of the wrong doer.
  e. A dishonest concealment of facts is also treated as a cheating.

Illustrations

The cheating offences re a explained using following Illustrations:

(a) A, by falsely pretending to be in the civil service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay. A cheats.

(b) A, by putting a counterfeit mark on an article, intentionally deceives Z into a belief that this article was made by a certain celebrated manufacturer, and thus dishonestly induces Z to buy and pay for the article. A cheats.

(c) A, by exhibiting to Z a false sample of an article, intentionally deceives Z into believing that the article corresponds with the sample, and thereby dishonestly induces Z to buy and pay for the article. A cheats.

(d) A, by tendering in payment for an article a bill on a house with which A keeps no money, and by which A expects that the bill will be dishonored, intentionally deceives Z, and thereby dishonestly induces Z to deliver the article, intending not to pay for it. A cheats.

(e) A, by pledging as diamonds articles which he knows are not diamonds, intentionally deceives Z, and thereby dishonestly induces Z to lend money. A cheats.

(f) A intentionally deceives Z into a belief that A means to repay any money that Z may lend him and thereby dishonestly induces Z to lend him money, A not intending to repay it. A cheats.

(g) A intentionally deceives Z into a belief that A means to deliver to Z a certain quantity of indigo plant which he does not intend to deliver, and thereby dishonestly induces Z to advance money upon the faith of such delivery. A cheats; but if A, at the time of obtaining the money, intends to deliver the indigo plant, and afterwards breaks his contract and does not deliver it, he does not cheat but is liable only to a civil action for breach of contract.

(h) A intentionally deceives Z into a belief that A has performed A's part of a contract made with Z, which he has not performed and thereby dishonestly induces Z to pay money. A cheats.

(i) A sells and conveys an estate to B. A, knowing that in consequence of such sale he has no right to the property, sells or mortgages the same to Z, without disclosing the fact of the previous sales and conveyance to B, and receives the purchase or mortgage money from Z. A cheats.

2.4.2.2 Punishment for Cheating

- The punishment for simple cheating is imprisonment which can be extend up to one year or fine or both.
- For the personating the punishment is imprisonment for a term which can be extend up to 3 years or with fine or both.
- If any person is deceived to deliver any property to any person then the punishment for that person is imprisonment for a term which can be extend up to 7 years with fine.

Syllabus Topic : Virus on the Internet

2.5 Virus on the Internet

Q. 2.5.1 Explain computer virus, damage and computer contaminant and mischief. (Ref. Sec.2.5) (5 Marks)

Computer Virus

- **Computer virus** means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource (Section 43,explanation (III)).
- Example of viruses are 'I love you' virus. The cousins of the virus and contaminants are bugs, worms, logic bombs and trojan horse. They destroy the computer systems, programs and the data residing therein.

Damage

- **"Damage"** means to destroy, alter, delete, add, modify or rearrange any computer resource by any means (Section 43, explanation (IV)).

Computer contaminant

- "Computer contaminant" means any set of computer instructions that are design to modify, destroy, record, transmit data or programs residing within a computer, computer system or computer network (Section 43,explanation(I)).

☞ The penalty and compensation

- If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network will be liable to pay damages by way of compensation not exceeding rupees one crore to the person affected (Section 43(c)).
- If any person, dishonestly or fraudulently, does any act referred to in Section 43(c), he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both (Section 66).
- The factors to be taken into account for determining quantum of compensation are the amount of gain of unfair advantage; the amount of loss caused the repetitive nature of the default. The act of planting virus and contaminants is amount to the criminal offence of mischief.

☞ Mischief (IPC 425)

- Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".

  Explanation 1 : It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause, wrong-ful loss or damage to any person by injuring any property, wheth-er it belongs to that person or not.

  Explanation 2 : Mischief may be committed by an act affecting property belonging to the person who commits the act, or to that person and others jointly.
- Mischief causing damage to the amount of fifty rupees. Whoever commits mischief and thereby causes loss or damage to the amount of fifty rupees or upwards, shall be punished with impris-onment of either description for a term which may extend to two years, or with fine, or with both (IPC 427).

Syllabus Topic : Defamation, Harassment and Email Abuse

2.6 Defamation, Harassment and Email Abuse

Q. 2.6.1 Explain defamation, harassment and email abuse. (Ref. Sec. 2.6) **(5 Marks)**

Q. 2.6.2 Explain the 10 exceptions of defamation. (Ref.Sec.2.6) (5 Marks)

- The freedom of speech and expression is given by the constitution of India is misused by few people. The criminal abuse of internet is min light in India.
- As internet is cost friendly and easily available many cases of defamation and harassments are reported. It has become a major cyber crime.
- There are websites available containing concocted nude photographs of Indian bollywood stars. So let's see what defamation, harassment is and email abuse:

Defamation

- Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person (IPC 499). In simple language defamation means damage done to the reputation of person.
- The imputation cannot be said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgrace-ful.
- If Meena is writing a letter to Neeta which is derogatory of Neeta it is not considered as defamation. But if Meena is writing a letter to Neeta which contains derogatory comments about Reema then it is considered as defamation.

Punishment

- The law provides that whoever prints or engraves any matter, knowing or having good reason to believe that such matter is defamatory of any person, shall be punished with simple imprisonment for a term which may extend to 2 years, or with fine, or with both (IPC 501).
- Publishers and the editors who publish the defamation matter are also liable for defamation. There are 10 exceptions, if imputation falls under this 10 exceptions then it won't be an offence of defamation.

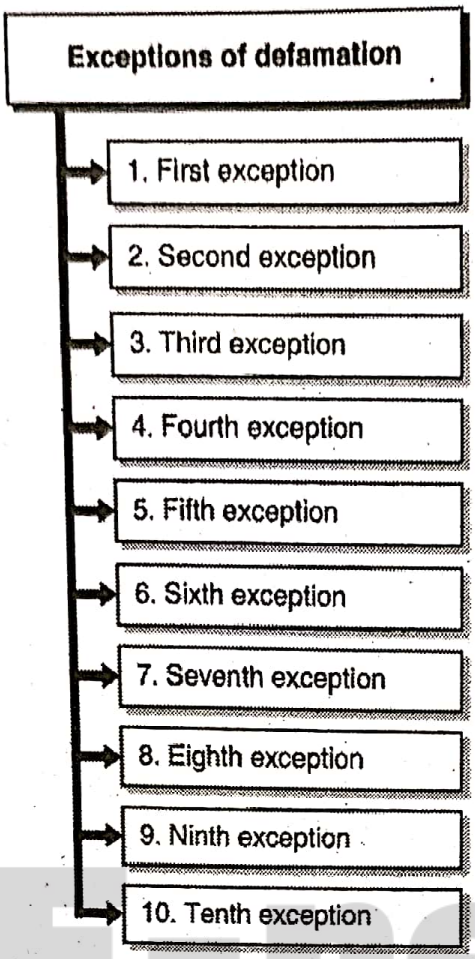

Fig. 2.6.1 : Exceptions of defamation

➜ 1. First exception

Imputation of truth which public good requires to be made or published. It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for the public good is a question of fact.

➜ 2. Second exception

Public conduct of public servants. It is not defamation to express in a good faith any opinion whatever respecting the conduct of a public servant in the discharge of his public functions, or respecting his character, so far as his character appears in that conduct, and no further.

➜ 3. Third exception

Conduct of any person touching any public question. It is not defamation to express in good faith any opinion whatever respecting the conduct of any person touching any public question, and respecting his character, so far as his character appears in that conduct, and no further.

☞ **Illustrations**

It is not defamation in A to express in good faith any opinion whatever respecting Z's conduct in petitioning Government on a public question, in signing a requisition for a meeting on a public question, in presiding or attending a such meeting, in forming or joining any society which invites the public support, in voting or canvassing for a particular candidate for any situation in the efficient discharges of the duties of which the public is interested.

➜ **4. Fourth exception**

Publication of reports of proceedings of courts. It is not defamation to publish substantially true report of the proceedings of a court of justice, or of the result of any such proceedings.

Explanation : A Justice of the peace or other officer holding an inquiry in open court preliminary to a trial in a court of Jus-tice, is a court within the meaning of the above section.

➜ **5. Fifth exception**

Merits of case decided in court or conduct of witnesses and others concerned. It is not defamation to express in good faith any opinion whatever respecting the merits of any case, civil or criminal, which has been decided by a court of justice, or respecting the conduct of any person as a party, witness or agent, in any such case, or respecting the character of such person, as far as his character appears in that conduct, and no further.

☞ **Illustrations**

(a) A says : "I think Z's evidence on that trial is so contradictory that he must be stupid or dishonest". A is within this exception if he says this is in good faith, in as much as the opin-ion which he expresses respects Z's character as it appears in Z's conduct as a witness, and no further.

(b) But if A says : "I do not believe what Z asserted at that trial because I know him to be a man without veracity"; A is not within this exception, in as much as the opinion which he express of Z's character, is an opinion not founded on Z's conduct as a witness.

➜ **6. Sixth exception**

Merits of public performance. It is not defamation to express in good faith any opinion respecting the merits of any performance which its author has submitted to the judgment

of the public, or respecting the character of the author so far as his character appears in such performance, and no further.

Explanation : A performance may be substituted to the judgment of the public expressly or by acts on the part of the author which imply such submission to the judgment of the public.

☞ **Illustrations**

(a) A person who publishes a book, submits that book to the judgment of the public.

(b) A person who makes a speech in public, submits that speech to the judgment of the public.

(c) An actor or singer who appears on a public stage, submits his acting or signing in the judgment of the public.

(d) A says of a book published by Z. "Z's book is foolish; Z must be a weak man. Z's book is indecent; Z must be a man of impure mind". A is within the exception, if he says this in good faith, in as much as the opinion which he expresses of Z respects Z's character only so far as it appears in Z's book, and no further.

(e) But if A says "I am not surprised that Z's book is foolish and indecent, for he is a weak man and a libertine". A is not within this exception, in as much as the opinion which he expresses of Z's character is an opinion not founded on Z's book.

➜ **7. Seventh exception**

Censure passed in good faith by person having lawful authority over another. It is not defamation in a person having over another any authority, either conferred by law or arising out of a lawful contract made with that other, to pass in good faith any censure on the conduct of that other in matters to which such lawful authority relates.

☞ **Illustrations**

A Judge censuring in good faith the conduct of a witness, or of an officer of the Court; a head of a department censuring in good faith those who are under his orders; a parent censuring in good faith a child in the presence of other children; a school master, whose authority is derived from a parent, censuring in good faith a pupil in the presence of other pupils; a master censuring a servant in good faith for remissness in service; a banker censuring in good faith the cashier of his bank for the conduct of such cashier as such cashier are within this exception.

8. Eighth exception

Accusation preferred in good faith to authorized person. It is not defamation to prefer in good faith an accusation against any person to any of those who have lawful authority over that person with respect to the subject matter of accusation.

Illustration

If A in good faith accuse Z before a Magistrate; if A in good faith complains of the conduct of Z, a servant, to Z's master; if A in good faith complains of the conduct of Z, and child, to Z's father A is within this exception.

9. Ninth exception

Imputation made in good faith by person for protection of his or other's interests. It is not defamation to make an imputation on the character of another provided that the imputation is made in good faith for the protection of the interests of the person making it, or of any other person, or for the public good.

Illustrations

(a) A, a shopkeeper, says to B, who manages his business "Sell nothing to Z unless he pays you ready money, for I have no opin-ion of his honesty". A is within the exception, if he has made this imputation on Z in good faith for the protection of his own interests.

(b) A, a Magistrate, in making a report of his own superior officer, casts an imputation on the character of Z. Here, if the imputation is made in good faith, and for the public good, A is within the exception.

10. Tenth exception

- Caution intended for good of person to who conveyed or for public good. It is not defamation to convey a caution, in good faith, to one person against another, provided that such caution be intended for the good of the person to whom it is conveyed, or of some person in whom that person is inter-ested, or for the public good.
- The cyber criminals having violent minds to threaten and intimidate others are punishable under IPC 503. The Indian Penal Code 503 explains criminal intimidation as follows:

Criminal intimidation

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit

to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intim-idation.

Explanation : A threat to injure the reputation of any deceased person in whom the person threatened is interested, is within this section.

Illustration : A, for the purpose of inducing B to desist from prosecuting a civil suit, threatens to burn B's house. A is guilty of criminal intimidation.

☞ Punishment for criminal intimidation (Section 506)

- The punishment for criminal intimidation is imprisonment of either description for a term which may extend to 2 years, or with fine, or with both.
- If threat be to cause either one of the following then the punishment is imprisonment up to 7 years, or with fine, or with both.
  - Death or grievous hurt, etc
  - If the threat be to cause death or grievous hurt,
  - Cause the destruction of any property by fire,
  - Cause an offence punishable with death or imprisonment for life, or with imprisonment for a term which may extend to 7 years,
  - To impute, unchastely to a woman, shall be punished with imprison-ment of either description for a term which may extend to 7 years, or with fine, or with both.
- There are many cases of email abuse, women harassment for taking the revenge are happening. So such cases are insulting the modesty of women.
- If any person insults the modesty of women, utters any word, makes any sound and gesture or intrudes the privacy of a woman then that person is punishable under Section 509.
- The punishment is simple imprisonment up to one year, or with fine, or with both.

Syllabus Topic : Cyber Pornography

2.7 Cyber Pornography

Q. 2.7.1 Explain cyber pornography. (Ref. Sec. 2.7) **(5 Marks)**

- Cyber pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional

pornographic content has now been largely replaced by online/digital pornographic content.

- Cyber pornography is banned in many countries and legalized in some. In India, under the Information Technology Act, 2000, this is a grey area of the law, where it is not prohibited but not legalized either.
- Under Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment up to 3 years and fine up to 5 lakhs :
  1. **Publication :** Which would include uploading on a website, what's app group or any other digital portal where third parties can have access to such content.
  2. **Transmission :** This includes sending obscene photos or images to any person via email, messaging, what's app or any other form of digital media.
  3. **Causing to be published or transmitted :** This is a very wide terminology which would end up making the intermediary portal liable, using which the offender has published or transmitted such obscene content. The intermediary guidelines under the information technology act put anonus on the intermediary/service provider to exercise due diligence to ensure their portal is not being misused.
- Section 67A of the Information Technology Act makes publication, transmission and causing to be transmitted and published in electronic form any material containing sexually explicit act or conduct, punishable with imprisonment up to 5 years and fine up to 10 lakhs.
- An understanding of these provisions makes the following conclusions about the law of cyber pornography in India extremely clear:
  1. Viewing cyber pornography is legal in India. Merely downloading and viewing such content does not amount to an offence.
  2. Publication of pornographic content online is illegal.
  3. Storing cyber pornographic content is not an offence.
  4. Transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence.

Syllabus Topic : Other IT Act Offences

2.8 Other IT Act Offences

Q. 2.8.1 Explain some IT offences and punishment for those offences. **(5 Marks)**
(Ref. Sec. 2.8)

The I.T. Act 2000 includes the following offences :

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of controller to give directions.
- Directions of controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Table 2.8.1

Section	Offence	Punishment
65	Tampering with computer source code	Imprisonment up to 3 years or fine up to ₹ 2 Lakhs.
66	Computer related offences	Imprisonment up to 3 years or fine up to ₹ 5 Lakhs.
66-A	Sending offensive message through communication device	Imprisonment up to 3 years and/or fine up to ₹ 1 lakh.
66-B	Dishonestly receiving stolen computer resource or communication device.	Imprisonment up to 3 years and/or fine up to ₹ 1 lakh.
66-C	Identify Theft	Imprisonment of either description up to 3 years and/or fine up to ₹ 1 lakh.
66-D	Cheating by personation by using computer resource.	Imprisonment of either description up to 3 years and/or fine upto ₹ 1 lakh.
66-Logical expression	Violation of privacy	Imprisonment up to 3 years and/or fine up to ₹ 2 lakh.
66-F	Cyber terrorism	Imprisonment extend to imprisonment for Life.

Section	Offence	Punishment
67	Publishing or transmitting obscene material in electronic form.	On first conviction, imprisonment up to 3 years and/or fine up to ₹ 5 Lakh. On subsequent conviction imprisonment up to 5 years and/or fine up to ₹ 10 Lakh.
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form.	On first Conviction imprisonment up to 5 years and/or find up to ₹ 10 Lakh on subsequent conviction imprisonment up to 7 years and/or find up to ₹ 10 Lakh.
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form.	On first conviction imprisonment of either description up to 5 years and/or fine up to ₹ 10 Lakh on subsequent Conviction imprisonment of either description up to 7 years and/or fine up to ₹ 10 Lakh.
67-C	Intermediary intentionally or knowingly contravening the directions about preservation and retention of information.	Imprisonment up to 3 years and fine.
68	Failure to comply with the directions given by controller.	Imprisonment up to 2 years and/or fine upto ₹ 1 Lakh.
69	Failure to assist the agency referred to in sub Section (3) in regard interception or monitoring or decryption of any information through any computer resource.	Imprisonment up to 7 years and fine.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource.	Imprisonment up to 7 years and fine.

Section	Offence	Punishment
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-Section (2) in regard monitor and collect traffic data or information through any computer resource for cyber security.	Imprisonment up to 3 years and fine.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70.	Imprisonment of either description up to 10 years and fine.
70-B	Indian computer emergency response team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc, who fails to prove the information called for a comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to ₹ 1 Lakh.
71	Misrepresentation to the controller to the certifying authority.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.
72	Breach of confidentiality and privacy.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.
72-A	Disclosure of information in breach of lawful contract.	Imprisonment up to 3 years and/or fine up to ₹ 5 Lakh.
73	Publishing electronic signature certificate false in certain particulars.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.
74	Publication for fraudulent purpose.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.

Syllabus Topic : Monetary Penalties, Adjudication and Appeals Under IT Act, 2000

2.9 Monetary Penalties, Adjudication and Appeals Under IT Act, 2000

Q. 2.9.1 Explain Monetary Penalties, Adjudication and Appeals Under IT Act, 2000. (Ref. Sec. 2.9) (5 Marks)

- IT Act provides certain contraventions for which a person has to pay for damages by the way of compensation or penalty. Section 43 of IT Act, 2000 is for penalty and compensation.
- It states that, if any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,

(a) Accesses or secures access to such computer, computer system or computer network [or computer resource];

(b) Downloads copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

☞ The following are the monetary penalties given by the IT laws Section 44

(a) For every failure to furnish any document, return or report to the controller or the certifying authority shall be liable to a penalty not exceeding 1.50 lakhs rupees.

(b) File any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding 5,000 rupees for every day during which such failure continues;

(c) If fail to maintain books of account or records, then he shall be liable to a penalty not exceeding 10,000 rupees for every day during which the failure continues.

- There is a separate adjudicating authority created for the adjudication of contraventions for which compensations are provided. The central government shall appoint any officer not below the rank of a director to the government of India or an equivalent officer of a state government to be an adjudicating officer for holding an inquiry in the manner prescribed by the central government.
- The adjudicating officer appointed shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed ₹ 5 crore: Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court.
- If evidence is produced related to the penalty to the adjudicating officer, he may order in writing to impose the penalty. Where more than one adjudicating officers are appointed, the central government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
- Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal and (Section 46 (3)(2)(4)(5), IT Act,2000).
- An adjudicating officer appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. No appeal shall file to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
- Every appeal shall be filed within a period of 45 days from the date on which a copy of the order made by the controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that the cyber appellate tribunal may entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was sufficient cause for not filing it within that period (Section 57(1)(2)(3), IT Act, 2000).

- Section 58 provides that, the Cyber Appellate Tribunal shall not be bound by the procedure laid down by the code of civil procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
- The Cyber Appellate Tribunal shall have same powers as are vested in a civil court under the Code of Civil Procedure. While trying a suit, in respect of the following matters, namely :
  (a) Summoning and enforcing the attendance of any person and examining him on oath;
  (b) Requiring the discovery and production of documents or other electronic records;
  (c) Receiving evidence on affidavits;
  (d) Issuing commissions for the examination of witnesses or documents;
  (e) Reviewing its decisions;
  (f) Dismissing an application for default or deciding it ex parte;
  (g) Any other matter which may be prescribed.
- **Section 61 provides that,** no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this act or the Cyber Appellate Tribunal constituted under this act is empowered by or under this act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this act.
- **Section 62 provides that,** any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the high court within 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order: Provided that the high court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.
- **Section 63 provides that,** any contravention may, either before or after the institution of adjudication proceedings, be compounded by the controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the controller or such other officer or the adjudicating officer may specify. Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this act for the contravention so compounded. Any contravention shall apply to a person who commits

the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

- No proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

Syllabus Topic : Network Service Providers

2.10 Network Service Providers

Q. 2.10.1 Who are the intermediaries? Explain in the responsibilities of intermediaries as per law. (Ref. Sec. 2.10) **(5 Marks)**

- Network service providers are the intermediary; the term network service is much wider than Internet Service Provider (ISP).
- Internet service providers give the network technology services to the internet users.
- The network service providers are of different types, internet access providers offers access to internet, Internet Service Provider offers additional services like hosting contents produced by themselves or by users or by third party, online service provider provides proprietary subscribers on their closed system. All the Internet service providers are network service providers but it is not correct vice versa.

☞ Who are the intermediaries?

The following are the intermediary.

1. Internet Service Provider (ISP).
2. Online services like Google, Facebook, and Twitter.
3. User generated content sites like Blogger, YouTube, and Flicker.
4. Internet café.
5. Hotel and restaurants.
6. University.
7. Workplace.

- Section 79 says that an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
- The provisions of subsection (1) are applied on the intermediary if; the job of intermediary is to provide access to communication system over which information made available by third parties.

- The information can be transmitted or temporarily stored or hosted. The intermediary does not- initiate the transmission, select the receiver of the transmission, and select or alter the information contained in the transmission.
- The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the central government may prescribe in this behalf.
- The provisions of subsection (1) are not applied on the intermediary if the intermediary has plotted, or assisted, or helped, or encouraged, whether by threats or promise or authorized in the commission of the unlawful act.
- If any link or data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Syllabus Topic : Jurisdiction and Cyber Crime

2.11 Jurisdiction and Cyber Crime

Q. 2.11.1 Write short note on Jurisdiction and Cyber Crime. (Ref. Sec. 2.11) **(5 Marks)**

- Section 1(2) in the Information Technology Act, 2000 has provided that act applies also to any offence or contravention there under committed outside India by any person. If the act involves a computer, computer system or computer network located in India.
  - If a website is created in UK which contains the pornographic material but it will not allow the IT Act jurisdiction to question the site. But if the maintenance of the website involves the computer system and the computer network located in India then the jurisdiction can have rights to ask questions. The Section 67 is applied on the website for cyber pornography.
  - If any county hacks computer, computer system or computer network in India then Section 66 of IT Act is applied.
  - If any person anywhere in the world plants Virus in computer system computer network located in India then the person is punishable under Section 43(c).
  - Section 75 of IT Act is only limited to those offences given therein and not to other offences under other laws like IPC, 1860.
  - Section 177 of the code of criminal procedure, 1973 provides the legal principle that

every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.

- When the place of the offence committed is unsure that is or where an offence is committed, partly in one local area and partly in another, or where an offence, is a continuing one, and continues to be committed in more local areas than one, or where it consists of several acts done in different local areas, it may be inquired into or tried by a court having jurisdiction over any of such local areas. The uncertainty of the place where the offence is committed is inquired by the jurisdiction (Section 178 crpc, 1973).
- When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such thing has been done or such consequence has ensued (Section 179 crpc, 1973).
- When an act is an offence by reason of its relation to any other act which is also an offence or which would be an offence if the doer were capable of committing an offence, the first- mentioned offence may be inquired into or tried by a court within whose local jurisdiction either act was done (Section 180 crpc, 1973).
- There are some offences which need to be inquired into or tried in some places. For example, any offence of criminal misappropriation or of criminal breach of trust may be inquired into or tried by a court within whose local jurisdiction the offence was committed or any part of the property which is the subject of the offence was received or retained, or was required to be returned or accounted for, by the accused person (Section 181 crpc, 1973).
- If any offence includes cheating, if the deception is practiced by means of letters or telecommunication messages, be inquired into or tried by any court within whose local jurisdiction such letters or messages were sent or were received. Additionally if any offence of cheating and dishonestly inducing delivery of property may be inquired into or tried by a court within whose local jurisdiction the property was delivered by the person deceived or was received by the accused person.(Section 182 crpc, 1973).
- If two or more courts have taken cognizance of the same offence and a question arises as to which of them ought to inquire into or try that offence, the question shall be decided by the high court under which jurisdictions both the court's function. If both courts are not subordinate to the same high court, then the question of jurisdiction will be decided by the high court within whose appellate criminal

jurisdiction the proceedings were first commenced (Section 186 crpc, 1973).

- The police officer or other person executing a warrant of arrest shall notify the substance there of to the person to be arrested, and, if so required, shall show him the warrant (Section 75 crpc, 1973).

Syllabus Topic : Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends

2.12 Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends

Q. 2.12.1 What are the strategies to tackle cyber crime and trends? (Ref. Sec. 2.12)(5 Marks)

– Cyber crimes have some characteristics which distinguishes it from the other forms of criminality.

- Technology is the main tool used to commit the cyber crime. Cyber criminals are the technocrats who are having the deep knowledge of internet and computers.
- Cyber crimes are very efficient as it operates and affects in no time. In few seconds any cyber crime can be committed, for example, hacking a website or doing a cyber fraud.
- Cyber crime can be performed from any place of globe. There are no geographical limitations and boundaries for cyber crime.
- Cyber criminals are invisible as cybercrime takes place in cyberspace. All the activities of cyber crime that is from preparation to execution takes place in cyberspace. As there is no geographical limitations then the degree of risk is low as compare to other traditional crimes.
- Cyber crimes cause harm and injury. It and destroys website which is created with huge investment. It also hacks confidential information for example defense system of the country. It also harms the economy by performing the scams.
- Cyber criminals are invisible so they can perform the cybercrime at the same time in different countries. Investigating the cyber crime is difficult as collecting evidence for cybercrime and proving it in the court of law is difficult.
- Cyber tools are easily and freely available in CD's and on internet, so, it is easy to commit cyber crimes.

- The IT Act, 2000 gives for most frequent and convenient methods used to deal with crime i.e. deterrence. Deterrent punishments strategy is used by the lawmakers to fight with crimes. To combat the crimes the law enforcement agencies in India uses third degree methods. But it is held illegal and violation of fundamental rights of a citizen by Supreme Court.
- Deterrent law is the only strategy to tackle the cyber criminality. Apart from deterrent law the following are the strategies used to deal with cyber crime.
- Strategies to be adopted to deal with cyber crimes :
  - Cyber crimes in world technology so it is necessary that the enforcement agencies should be trained in intricacies of technology it will be helpful conduct the investigations effectively. The cyber corps should be competent for cyber crime investigation. The cyber Corps should learn the tools like trace and trap devices to detect cyber crime.
  - As we know cybercrime have no geographical limitations and the cyber criminals jumps the geographical borders know as jurisdictional jumping. So it is important to have cooperation between law enforcement agencies of different countries.
  - Effective laws of extradition and their implementation are necessary to bring to trial cyber criminal across borders. The existing extradition treaties ought to be strengthened by corporation in the international community.
  - Make the use of encryption and other security technologies.
  - IT Industries should not be depend upon the law enforcement agencies for tracking the cyber criminal, they have to take the responsibility of protecting their own computer system and networks by using the secure technologies.
  - Government has to encourage secure technologies. They have to work with private sectors in partnership. Government should encourage research and development in security technologies. Funding and support should be given by government to R&D and give the education about the measures to counter cybercrimes.
  - There are many cyber crimes which are not reported by the victims because of the fear of loss in business and losing the confidence of customers. But it is important to understand that suppressing information about having victimized encourages cyber crime. So, to understand the different forms of cyber crime it is must for private sectors to share the information about cyber crime.
  - There should be easy identification of the netizens. But this identification should be

carried out when investigating alleged into a cyber crime. Identification should be allowed but the disclosure of the identification is regulated and allowed only in exceptional circumstances. So it the right of disclosure is not misused, deterrent penalties can be prescribed.

Syllabus Topic : Criminal Justice in India and Implications on Cyber Crime

2.13 Criminal Justice in India and Implications on Cyber Crime

Q. 2.13.1 Explain Criminal Justice In India and Implications on Cyber Crime. (Ref. Sec. 2.13) (5 Marks)

1. In India there are always delay in criminal and civil justice system. The following are the reasons behind the delays :
   - Increase in population.
   - Negligence by the government.
   - Lack of responsibility and sensitivity and the slow attitude.
   - Uneven ratio between the number of cases and the number of judges.
2. Apart from delayed criminal justice there are two trends in our criminal justice system which are going unnoticed.
   - The Judiciary is leaning towards convictions and it results in rising crimes in society. There are hardened criminals if too much emphasis is given on protection of their fundamental and human rights then such criminals will go free without exposing any element of criminality then the crime will get unpunished and the society will suffer. The society expects that the police must deal with the criminals in effective and efficient manner but the above given observations affects the efficiency of the police.
   - The Judiciary should be strict against the grant of bail, but the bail cannot be denied as a matter of punishment. The useful principal regarding the law of bail is "bail not jail".
   - This principle is not applied in practice; the courts are influenced by provision which is labelled on the accused by the prosecution. The Judgment regarding granting the bail is not exercised liberally.
   - The media is also responsible for this as they are giving wide coverage to criminal cases and thus gives an impression before the start of the trial.

3. Recently in Place of TADA (Terrorist and Disruptive Activities Act) government proposed a law. This long permits restriction on granting the bail, to penalize journalist for having information about terrorists, Burden is shifted on accused to prove his innocence.

- The trend towards deterrence by leaning towards convictions, strictness in the grant of bail and legislative measures would have serious implications on cyber crime cases especially for those accused of committing cyber crimes.
- In many cyber crime cases there are delay in investigation and trial of cyber crimes as witnesses are scattered over different and faraway lands leading to time consuming investigation and trials are tending towards conviction, strictness for granting the bail and the hype created by the media over cyber crime would seriously injustice those accused of the cybercrime. Such under trials are likely to be the new victims of the cyber crime.

2.14 Exam Pack (University Questions)

☞ **Syllabus Topic : Concept of 'Cyber Crime' and the IT Act, 2000**

Q. 1 What is cyber crime? How the classification of cyber crime is done? (Refer Section 2.1) **(5 Marks)**

Q. 2 Explain the term Document and Electronic record. (Refer Section 2.1) **(5 Marks)**

☞ **Syllabus Topic : Hacking**

Q. 3 What is hacker? What are the different types of hackers? (Refer Section 2.2) **(5 Marks)**

Q. 4 Explain how IT act defines and publishes hacking. What is the punishment for hacking? (Refer Section 2.2) **(5 Marks)**

☞ **Syllabus Topic : Teenage Web Vandals**

Q. 5 Explain teenage web vandals. (Refer Section 2.3) **(5 Marks)**

☞ **Syllabus Topic : Cyber Fraud and Cyber Cheating**

Q. 6 Explain cyber fraud and cyber cheating. (Refer Section 2.4) **(5 Marks)**

☞ **Syllabus Topic : Virus on the Internet**

Q. 7 Explain computer virus, damage and computer contaminant and mischief. (Refer Section 2.5) **(5 Marks)**

Syllabus Topic : Defamation, Harassment and E-mail Abuse

Q. 8 Explain defamation, harassment and email abuse. (Refer Section 2.6) **(5 Marks)**

Q. 9 Explain the 10 exceptions of defamation. (Refer Section 2.6) **(5 Marks)**

Syllabus Topic : Cyber Pornography

Q. 10 Explain cyber pornography. (Refer Section 2.7) **(5 Marks)**

Syllabus Topic : Other IT Act Offences

Q. 11 Explain some IT offences and punishment for those offences. (Refer Section 2.8) **(5 Marks)**

Syllabus Topic : Monetary Penalties, Adjudication and Appeals Under IT Act , 2000

Q. 12 Explain Monetary Penalties, Adjudication and Appeals Under IT Act, 2000. (Refer Section 2.9) **(5 Marks)**

Syllabus Topic : Network Service Providers

Q. 13 Who are the intermediaries? Explain in the responsibilities of intermediaries as per law. (Refer Section 2.10) **(5 Marks)**

Syllabus Topic : Jurisdiction and Cyber Crime

Q. 14 Write short note on Jurisdiction and Cyber Crime. (Refer Section 2.11) **(5 Marks)**

Syllabus Topic : Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends

Q. 15 What are the strategies to tackle cyber crime and trends? (Refer Section 2.12) **(5 Marks)**

Syllabus Topic : Criminal Justice In India and Implications On Cyber Crime

Q. 16 Explain Criminal Justice In India and Implications on Cyber Crime. (Refer Section 2.13) **(5 Marks)**

Chapter Ends...

❑❑❑