Information Technology Act, 2000 (India):

- The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000.
- This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.
- The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 94 sections.
- The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

5.1.1 Salient Features of I.T Act

The salient features of the I.T Act are as follows :

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

5.1.3 Cyber Law Offence and Punishments

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

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

5.1.2 Scheme of I.T Act

The following points define the scheme of the I.T. Act :

- The I.T. Act contains 13 chapters and 90 sections.
- The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
- It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
- Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
- Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
- Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.

Cyber-crime usually includes the following :

(1) Unauthorized access of the computers
(2) Data diddling
(3) Virus/worms attack
(4) Theft of computer system
(5) Hacking
(6) Denial of attacks
(7) Logic bombs
(8) Trojan attacks
(9) Internet time theft
(10) Web jacking
(11) Email bombing
(12) Salami attacks
(13) Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows :

(i) Tampering with the computer source documents.
(ii) Hacking with computer system.
(iii) Publishing of information which is obscene in electronic form.
(iv) Power of Controller to give directions.
(v) Directions of Controller to a subscriber to extend facilities to decrypt information.
(vi) Protected system.
(vii) Penalty for misrepresentation.
(viii) Penalty for breach of confidentiality and privacy.
(ix) Penalty for publishing Digital Signature Certificate false in certain particulars.
(x) Publication for fraudulent purpose.
(xi) Act to apply for offence or contravention committed outside India Confiscation.
(xii) Penalties or confiscation not to interfere with other punishments.
(xiii) Power to investigate offences.

Offence and penalties against Information Technology Act. 2000

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
			Congizability
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
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 fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC

67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
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	Offence is Non-Bailable, Cognizable.
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	Offence is Non-Bailable, Cognizable.
69-B 69-C	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 cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.

5.1.4 Application of the I.T Act

As per the sub clause (4) of Section 1, nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply :

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- **A power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- **A trust** as defined in section 3 of the Indian Trusts Act, 1882;
- **A will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- **Any contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government

5.2 CYBERCRIME AND CRIMINAL JUSTICE : PENALTIES

GQ. What is cybercrime? Mention related penalties.

What is Cybercrime ?

- The crime that involves and uses computer devices and Internet is known as **cybercrime**.
- Cybercrime can be committed in opposition to an individual or a group; it can also be committed against government and private organizations. It may be planned to harm someone's reputation, physical harm, or even mental harm.
- Cybercrime can cause direct harm or indirect harm to whoever the sufferer is.
- However, the largest threat of cybercrime is on the financial security of an person as well as the government.

- Cybercrime causes loss in billions each year.
- Cyber terrorists typically use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information.
- Internet is one of the way by which the offenders can gain such price sensitive information of companies, firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling unlawful articles, pornography etc.
- This is done through many methods such as phishing, spoofing, pharming, internet phishing, wire transfer etc. and use it to their own advantage without the permission of the individual.
- Many banks, financial institutions, investment houses, brokering firms etc. are being victimized and endangered by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages.

Many of the cyber-crimes penalized by the IPC and the IT Act have the same ingredients and terminologies.

(i) Hacking and Data Theft

- Sections 43 and 66 of the IT Act penalise a number of activities vary from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, destroying information residing in a computer etc.
- The maximum penalty for the above offences is penal servitude of up to 3 years or a fine or Rs. 5,00,000 or both.

i) Receipt of stolen property

- Section 66B of the IT Act command penalty for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property custody to have done so dishonestly or should have reason to believe that it was stolen property.
- The punishment for this offence under Section 66B of the IT Act is durance of up to 3 years or a fine of up to Rs. 1,00,000 or both.

iii) Identity theft and cheating by personation

- Section 66C of the IT Act states that penalty for identity theft and provides that anyone who crooked or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with durance of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1,00,000.

(iv) Obscenity

- Sections 67, 67A and 67B of the IT Act states that, penalty for publishing or transmitting, in electronic form : (i) obscene material; (ii) material containing sexually explicit act, and (iii) material depicting children in sexually explicit act, etc. respectively.
- The penalizing for an offence under section 67 of the IT Act is, on the first conviction, durance of either description for a term which may extend to 3 years, to be accompanied by a fine which may extend to Rs. 5,00,000, and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 years, to be accompanied by a fine which may extend to Rs. 10,00,000.

Adjudication and Appeals Under the IT Act, 2000:

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 in-charge of a computer, computer system or computer network.

a. Accesses or secures access to such computer, computer system, 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.

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 lakh 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.

--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.

⏱IT Act. 2008 and its Amendments:

⏭ 5.4 IT ACT. 2008 AND ITS AMENDMENTS

GQ. Explain in detail IT Act. 2008 and its Amendments.

- According to Ministry of Communication and Information Technology, IT Act. 2008 has come to effect from 27 October 2009. This Act has received both good or bad response.
- The IT Act. 2008 has been discuss since it was passed by the Indian Parliament in December 2008, about a month after the terrorist attacks in Mumbai.
- Special sections like Section 69 which provides power to the Indian government for interception, monitoring, decryption and blocking electronic data traffic have come under major criticism.
- By using the Indian IT Act 2008, provide with Section 3A any electronic record or electronic signature or electronic authentication technique shall be reliable if and only if :
  - The signature creation data or the authentication data are same in the context they used it should not be create by another person.
  - Any alteration to the electronic signature after affixing such electronic signature is detectable.
  - Any alteration made to the information provided after affixing the electronic signature is detectable. Here the integrity of the message is checked because when sender sends the electronic document over insecure channel before it reaches to intended receipts if contents of message are changed then it invalidate the principle of integrity.

- Government of India now decided under Indian IT Act law 2008 law to introduce the concept of electronic signature for the purpose of Information Technology, cyber laws, business transactions and communication.
- The new IT act lacks coverage of areas like social networking, user generated content, spyware and malware. "Emerging cybercrimes and mobile crimes have not been appropriately addressed. The definition of sensitive and personal data has been left to the government," says Duggal.
- Yet another bone of contention in the new IT Act is the reduction in punishment tenures for cybercrime. Although the new IT Act rates cyber terrorism as a heinous offence punishable with life imprisonment, it is a cybercrime friendly legislation, claims Duggal.
- The IT Act has reduced its quantum of punishment and almost all cyber crimes are now bailable. "An offense such as online obscenity earlier received an imprisonment for five years. Now it has been reduced to a year," observes Duggal.
- To sum it up, the new Indian IT Act tries to capture several aspects dealing with personal data privacy, Blackhat hacking and cyber terrorism. However, a strong and regulated implementation mechanism is required to mitigate possibilities of the Act's misuse.

5.4.1 The Indian IT (Amendments) Act-Challenges

GQ. Write short note on Indian IT Act challenges.

- Whatever the IT act laws defined in earlier section are important as far as cyber security is concern. But what is challenge today in front of India is how to tackles all this cyber crimes.
- As India is growing economically very fastly with the same speed the usage of e-governance also increasing because everything now a day is online. It is quite obvious that usage increases the number of cyber crimes. Cybercrimes are increasing because of email shopping, pornography, Denial of Service attacks, illegal access of data and many more.
- With in India Section 43A and 72 A of the Information Act provides protection to data. If we want to transfer data outside India one cannot seek protection under these sections.
- Cyber security in India is not upto the mark and India has no cyber security policy and strategy that can be implemented under any legal framework.

- Frankly mentioning that India has designed a cyber security policies and Laws is not enough to tackle the cyber crimes (weak and ineffective in tackling the fast growing cyber crimes in India).
- India having only two Information Technology Act incorporated, i.e. IT Act 2000 and amendment Act 2008. Because of inefficient laws India has face many cyber attacks in past and in present like Indian websites are regularly hacked by an attacker, sensitive data of ministries has been stolen.
- What is challenge in front of India is to make cyber laws more robust, strong and legally sound which will take immediate decisions. Many cyber crime cases are pending because of fewer resources, manpower unavailability etc.
- One of the major challenge in front of India is to protect sensitive data of private companies, firms (BPO) because these companies have all kind of employee data such as financial details, account number, credit card details, personal data of individuals across the world and even their medical history also.
- Companies store all this data in electronic form and could be vulnerable or misused by the companies and employees. However, the provision made in India IT Act 2008 can't meet the needs of corporate India and not provide proper solution to data protection.

How to overcome these challenges ?

- Requires strong Indian IT Act laws to control cyber crimes.
- There should be ban on pornography sites as it is now government is taking these points into consideration.
- We have habit to send and upload all photographs on social site like facebook, twitter which is harmful because anybody morph that images and may publish on different sites of worldwide web.
- Always use strong antivirus as it helps to protect malwares, virus, worms and spywares.
- Never share our credential with unknown person.
- Keep watch on children which games they are playing on Internet most of virus and attacks happen because of online gaming. It also slows down the machine speed.