Module 6

Cyber laws

- The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce.
- All these governing mechanisms and legal structures come within the domain of Cyber law.

  Cyber law is important because it touches almost all aspects of transactions and activities and on involving the internet, World Wide Web and cyberspace.
- Every action and reaction in cyberspace has some legal and cyber legal angles.

Cyber laws

- Cyber Crime is not defined in Information Technology Act 2000 nor in the National Cyber Security Policy 2013 nor in any other regulation in India.
- Hence, to define cyber-crime, one can say, it is just a combination of crime and computer. In other words ‘any offence or crime in which a computer is used is a cyber-crime’.
- Even a petty offence like stealing or pick pocket can be brought within the broader purview of cybercrime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster.
- The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime.

- Cyber law encompasses laws relating to:
- · Cyber crimes
  · Electronic and digital signatures
  · Intellectual property
  · Data protection and privacy

  Cyber space includes computers, networks, softwares, data storage devices(such as hard disks, USB disks etc), the internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.
  Cyber Crime?
- # Any crime with the help of computer and telecommunication technology.
  # Any crime where either the computer is used as an object or subject. [1]

- Categories of Cyber Crime
- 1. Cybercrimes against persons
  2. Cybercrimes against property
  3. Cybercrimes against government

1. Against a Person
Cyber stalking
Impersonation
Loss of Privacy
Transmission of Obscene Material
Harassment with the use of computer

2. Against Property
Unauthorized Computer Trespassing
Computer vandalism
Transmission of harmful programmes
Siphoning of funds from financial institutions
Stealing secret information & data
Copyright

3. Against Government
Hacking of Government websites
Cyber Extortion
Cyber Terrorism
Computer Viruses[2]

Need For Cyber Law

- In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes.
- Internet was initially developed as a research and information sharing tool and was in an unregulated manner.
- As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc.
- All legal issues related to internet crime are dealt with through cyber laws.
- As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.
- In today's highly digitalized world, almost everyone is affected by cyber law.

Cyber Laws In India

- In India, cyber laws are contained in the Information Technology Act, 2000 (“IT Act”) which came into force on October 17, 2000.
- The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

  The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace.
- In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.

Cyber Laws In India

- None of the existing laws gave any legal validity or sanction to the activities in Cyberspace.
- For example, the Net is used by a large majority of users for email. Yet till today, email id not “legal” in our country.
- There is no law in the country, which gives legal validity, and sanction to email.
- Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament.
- As such the need has arisen for Cyber law.

Importance of Cyber Laws

- We are living in highly digitalized world.
- All companies depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in “non-cyber crime” cases, important evidence is found in computers/ cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.
- Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber law is extremely important.[4]

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 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.
- **The IT Act, 2000 has two schedules:**
- **First Schedule –**
  Deals with documents to which the Act shall not apply.
- **Second Schedule –**
  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

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

Section and Punishment

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine or Rs. 10,00,000 or both.

The Information Technology Amendment Act, 2008

- The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000).
- The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In).
- The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime.
- The Act also sought to foster security practices within India that would serve the country in a global context.
- The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

The Information Technology Amendment Act, 2008

- Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.
- The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals.
- Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion. According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India, "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic.
- The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state."