Cyber Law And Internet Security - Syllabus

Unit-1

Cyber Space Jurisdiction: Jurisdiction issues under IT Act, 2000, traditional principals of jurisdiction,

extra-terrestrial jurisdiction and case laws on cyber space jurisdiction.

E–commerce and Laws in India: Digital / Electronic signature in Indian laws, E–commerce; issues

and provisions in Indian law, and E –Governance.

Unit-2

Intellectual Property Rights, Domain Names and Trademark Dispute: Concept of trademarks in

internet era, cybersquatting, reverse hijacking, jurisdiction in trademark disputes, copyright in the

digital medium, and copyright in computer programs

Unit-3

Developing Secure Information Systems: Information security governance & risk management,

security architecture & design security issues in hardware, data storage & downloadable devices,

physical security of IT assets, access control, CCTV and intrusion detection systems and backup

security measures.

Unit-4

Security Policies: Development of policies, WWW policies, email security policies, policy review

process-corporate policies-sample security policies, publishing and notification requirement of the

policies.

Que1. What is cyber space ?

cyberspace is an unreal world where information is constantly transmitted through or between computers.

History of the word- Cyber Space

The term Cyber Space was introduced by William Gibson in his book “Neuromancer” in 1984. It is still used worldwide to describe facilities or features that are linked to internet .

Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information, systems that support our companies, infrastructure and services.

2. Cyberspace can be divided into a multi-layer model comprised of:

1. Physical foundations: such as land and submarine cables, and satellites that provide communication pathways, along with routers that direct information to its destination.

2. Logical building blocks: including software such as smartphone apps, operating systems, or web browsers, which allow the physical foundations to function and communicate.

3. Information: that transits cyberspace, such as social media posts, texts, financial transfers or video downloads. Before and after transit, this information is often stored on (and modified by) computers and mobile devices, or public or private cloud storage services.

4. People: that manipulate information, communicate, and design the physical and logical components of cyberspace.

The four layers of cyberspace described above (**physical, logical, information, and people**) have three primary characteristics—**connectivity, speed and storage.**

Que3. Is Cyberspace the same as the Internet ?

Cyberspace and the internet have been capable of creating a virtual world for cultural as well as for various social practices. With virtual cyberspace reality, it is now possible to see, communicate, and represent information. The cyberspace internet is a virtual world of

computers that facilitates communication online. It is a world where information gets transmitted through the internet. **Cyberspace internet is however different from the internet.** The internet is a global network of computers that offers information and facilitates communication through the networks that are interconnected. This it does by using standardized communication protocols.

The cyberspace internet on the other hand is the virtual world of computers which is the world over a virtual computer network environment.

To understand the cyberspace meaning and its differences clearly it can be said that the internet is a set of networks of computers that make use of the internet protocol to communicate. This is the internet. Cyberspace is an information world through the internet.

Que4. What are the Laws Defining Cyber Laws?

The laws prevailing the area of cyber space and the world of the internet is cyber law and the users of the areas fall within the ambit of these cyber laws.

cyber law is essentially the branch of law that deals with legal issues which are related to use of inter-networked information technology. The governing mechanism and legal structures that oversee the growth of electronic commerce in India fall within the domain of cyber law.

Cyber law essentially encompasses laws relating to electronic and digital signatures, cybercrimes, intellectual property, data protection and privacy . The major areas of cyber laws includes fraud, copy right harassment or stalking , trade secrets freedom of speech, contracts and employment law.

Regulation and legislation in India

Due to the increase in globalization, computerization and the growth of e-commerce in 90s, **UNCITRAL** adopted its **Model Law on e-commerce in 1996**. So In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries. Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. **The UN General Assembly** then passed a resolution in 1997 recommending the states in the **UN** to give favourable considerations to the model Law. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

In the IT Act, 2000, there are special provisions under Chapter III to grant legal recognition to electronic records, signature, and also encourage the government and its agencies to use them.

Q 5: What is Need for Cyber Law?

Answer: There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1) Cyberspace is an **intangible** dimension that is impossible to govern and regulate using conventional law.

2) Cyberspace has complete **disrespect for jurisdictional boundaries**.

3) Cyberspace handles **gigantic traffic volumes every second**. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4) Cyberspace is absolutely **open to participation by all**.

5) Cyberspace offers **enormous potential for anonymity** to its members.

6) exchanged between cyber-citizens.

7) Cyberspace offers never-seen-before **economic efficiency**. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

8) Electronic information has become the main object of cyber crime. It is characterized by **extreme mobility**, which exceeds by far the mobility of persons, goods or other services.

International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

9) A software source code worth crores of rupees or a movie can be **pirated across the globe** within hours of their release.

10) **Theft of** corporeal **information** (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly

Explain IT Act 2000 in detail.

The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce.

- The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime.
- Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged.
- The law prescribes penalties for various cybercrimes and fraud through digital/electronic format.
- It also gives legal recognition to digital signatures.
- The IT Act also amended certain provisions of the Indian Penal Code (IPC), the Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872 and the Reserve Bank of India Act, 1934 to modify these laws to make them compliant with new digital technologies.
- In the wake of the recent Indo-China border clash, the Government of India banned various Chinese apps under the Information Technology Act.

Explain various jurisdictional issues under IT Act 2000.

The Information Technology Act, 2000 ("**IT Act**") sets out a framework for resolution of disputes arising out of cyber-attacks like hacking, data theft, and phishing.The framework allows victims of such attacks to claim damages and compensation from the attackers. Cybercrimes are mostly dealt with by '**cybercrime cells**' of the respective police departments. In addition to briefly discussing the the issues of jurisdiction and applicable law Jurisdiction .Jurisdiction is the authority by which courts take cognisance of and decide cases. The word jurisdiction is of large and comprehensive import, and embraces every kind of judicial action. Jurisdiction for our purpose is broadly of two types: .

1. Subject matter jurisdiction

2.Personal jurisdiction

Cyber Space Jurisdiction

Jurisdiction gives power to the appropriate court to hear a case and declare a judgment. In cybercrime instances, the victim and the accused are generally from different countries, and hence deciding which cyber jurisdiction will prevail is conflicting. The internet as stated earlier has no boundaries; thus, no specific jurisdiction in cyberspace can be titled over its use. A user is free to access whatever he wishes to and from wherever he wishes to. Till the time a user's online activity is legal and not violative of any law, till then there is no issue. However, when such actions become illegal and criminal, jurisdiction has a crucial role to play.

For example, if a user commits a robbery in country 'A' while sitting in country 'B' from the server of the country 'C,' then which country's jurisdiction will apply needs to be answered. In this case, the transaction might have been done virtually, yet the people are present physically in their respective countries governed by their laws and the court generally decides the cyber jurisdiction of the country where the crime has been actually committed.

In cyberspace, there are generally three parties involved in a transaction: the user, the server host, and the person with whom the transaction is taking place, with the need to be put within one cyberspace jurisdiction.All three parties in this illustration belong to three different countries, now the laws of 'A,' 'B' or 'C' will be prevalent or not, or even municipal laws will be applicable or international laws the issues of jurisdiction in cyberspace. The extent of a court's competency to hear a cross-border matter and apply domestic state laws is another issue.

Types of Cyberspace jurisdiction

There are three types of cyber jurisdiction recognized in international law, namely-

- **Personal Jurisdiction** – It is a type of jurisdiction where the court can pass judgments on particular parties and persons.
- **Subject-matter jurisdiction** – It is a type of jurisdiction where the court can hear and decide specific cases that include a particular subject matter. For instance, a complaint regarding a consumer good should be filed in the district consumer forum rather than district court as district consumer forums specifically look at consumer-related cases. In the same manner, all environmental-related cases are tried in NGT rather than a district court.
- **Pecuniary Jurisdiction** – This type of jurisdiction mainly deals with monetary matters. The value of the suit should not exceed the pecuniary jurisdiction. There are various limits set for a court that can try a case of a certain value beyond which it is tried in different courts.

Jurisdiction under Information Technology Act, 2000

Information Technology Act, 2000 in section 1(2) states that the Act extends to the whole of India and applies also to any offence or contravention thereunder committed outside India by any person.

Further, "Section 75 states that subject to the provision of sub-section (2), the provision of this act shall also apply to any offence or contravention committed outside India by any person irrespective of his nationality. For the purpose of subsection (1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constitutes an offence or contravention that involves a computer, computer system, or computer network located in India."

This provides prescriptive cyberspace jurisdiction in India, and any act committed violative of this Act in India by a resident, or a non-resident will be punishable.

What does IT Act 2000 legislation deals with?
The Act essentially deals with the following issues:
 Legal Recognition of Electronic Documents
 Legal Recognition of Digital Signatures
 Offenses and Contraventions
 Justice Dispensation Systems for cyber crimes.

Why did the need of IT Amendment Act 2008 (ITAA) arise?
The IT Act 2000, being the first legislation on technology, computers, e-commerce and e-communication, the was the subject of extensive debates, elaborate reviews with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some obvious omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the IT Act also being referred in the process with the reliance more on IPC rather on the ITA.
Thus the need for an amendment – a detailed one – was felt for the I.T. Act. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analysed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the **Information Technology Amendment Act 2008** was placed in the Parliament and passed at the end of 2008 (just after Mumbai terrorist attack of 26 November 2008 had taken place). The IT Amendment Act 2008 got the President assent on 5Feb 2009 and was made effective from 27 October 2009.

Q6. What are features of IT Act 2000?
Notable features of the ITAA 2008 are:
- Focussing on data privacy
- Focussing on Information Security

- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism

Digital Signature under the IT Act, 2000

Digital signature means authentication of any electronic record by a subscriber

by means of an electronic method or procedure in accordance with the provisions of section 3. Section 3 deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two definite steps.

First, the electronic record is converted into a message digest by using a mathematical function known as 'Hash function' which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public

key to identify the originator of the message.

31'Hash function' means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computation-ally infeasible to derive or reconstruct the original electronic record from the hash result produced by the algorithm; that two electronic records can produce the same hash result using the algorithm.

Digital signatures are a means to ensure validity of electronic transactions however who guarantees about the authenticity that such signatures are indeed valid or not false. In order that the keys be secure the parties must have a high degree of confidence in the public and private keys issued.

Digital Signature is not like our handwritten signature. It is a jumble of letters and digits. It looks something like this.

----- BEGIN SIGNATURE----

Uz5xHz7DxFwvBAh24zPAQCmOYhT47gvuvzO0YbDA5txg5bN1Ni3hgPgnRz8Fw

xGU

oDnj7awl7BwSBeW4MSG7/3NS7oZyD/AWO1Uy2ydYD4UQt/w3d6D2Ilv3L8EO

iHiH +r5K8Gpe5zK5CLV+zBKwGY47n6Bpi9JCYXz5YwXj4JxTT+y8=gy5N

----- END SIGNATURE ------

Digital signature vs. electronic signature

While *digital signature* is a technical term, defining the result of a cryptographic process that can be used to authenticate a sequence of data, the term electronic signature or *e-signature* is a legal term that is defined legislatively.

Electronic governance (e-governance) is the most treasured instrument with the government to provide public services in an accountable manner. Unfortunately, in the current scenario, there is no devoted legal structure for e-governance in India.

Similarly, there is no law for obligatory e-delivery of public services in India. And nothing is more hazardous and troublesome than executing e-governance projects without sufficient cybersecurity. Hence, securing the e-governance services has become a crucial task, especially when the nation is making daily transactions through cards.

Fortunately, the Reserve Bank of India has implemented security and risk mitigation measures for card transactions in India enforceable from 1st October, 2013. It has put the responsibility of ensuring secured card transactions upon banks rather than on customers.

"E-government" or electronic government refers to the use of Information and Communication Technologies (ICTs) by government bodies for the following −

- Efficient delivery of public services
- Refining internal efficiency
- Easy information exchange among citizens, organizations, and government bodies
- Re-structuring of administrative processes.

E -commerce is a method of conducting business electronically rather than through traditional physical means. This includes all internet-based retail activities such as purchasing goods, receiving services, delivery, payment facilitation, and supply chain and service management. Get to know about the E-Commerce Laws and Regulations in India.

Growth of E-Commerce

Government initiatives such as Startup India, Digital India, the allocation of funds for the BharatNet Project, the promotion of a "cashless economy," and the launch of the Unified Payment Interface by the RBI and the National Payment Corporation of India have all ontributed to the country's e-commerce sector's growth and success.

Applicable Laws & Regulations

Regulatory

1. Foreign Direct Investment Policy
2. Further, the Foreign Exchange Management Act, 1999 Companies Act, 2013
3. Payment and Settlement Act, 2007 and other RBI regulations on payment mechanisms
4. Labelling and Packaging
5. Legal Metrology Act, 2009 read with Legal Metrology (Packaged Commodity) Rules, 2011
6. Sales, Shipping, Refunds and Returns
7. Moreover, Regulations prescribed by the relevant ministry/state regulations

Technology & Data Protection

1. Information Technology Act, 2000
2. Additionally, Information Technology (Intermediaries Guidelines) Rules, 2011
3. Information Technology Act, 2000 (IT Act) and General Data Protection Regulations (GDPR).
4. Consumer Protection Act, 1986