

UNIT 162 – UPSC - Cyber Laws

In technology driven society, internet has huge contribution for the growth of humans. Many investigators explained that cyberspace is a physical space but actually were a computer-generated construction representing abstract data. It is a virtual medium. It has no boundaries, no geographical mass, or gravity. Numerous advancements are done due to cyber activities but the major question is that whether it should be regulated or not. Cyber Law is the law that controls cyber space. Cyber space is a very broad term and includes computers, networks, software, and data storage devices such as hard disks, USB disks, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines. The increased dependence of individuals and organizations on cyberspace has resulted in many cybercrimes.



Cyber crimes are illegal acts where the computer is used either as a tool or a target or both. The massive growth in electronic commerce (e-commerce) and online share trading has led to an unusual erupt in incidents of cybercrime. Although, there is system to protect devices from infected with computer virus to the data and computer networks such as firewalls, antivirus software, and other technological solutions, but in India efforts must be done towards effective use of these technologies to protect the valuable data and to combat cyber-crime. Even expert users of IT tools may not be aware of cyber victimization. Along with the progression in technology it is similarly important to be aware of cyber-crime and other related issues thereof. The cyber safety depends on the knowledge of the technology and the care taken while using internet and that of the defensive measures adopted by user and servers systems. Cyber law portrays the legal issues associated with the use of communications technology, mainly "cyberspace", i.e. the Internet. It is a junction of numerous legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. It is established that cyber law applies to regulations designed for the physical world, to human activity on the Internet. Cyber law basically deals with almost all aspects of transaction and activities concerning Internet, World Wide Web and Cyberspace in India.

The law for cyberspace is to control the man and the machine. The fundamental goal of cyber laws is to legalize human behaviour and not technology. Cyber laws are technology intensive laws, advocating the use but not the mishandling of technology. Cyber law comprises of all the cases, statutes and legal provisions that affect persons and institutions who control the entry to

cyberspace, provide access to cyberspace, create the hardware and software which enable people to access cyberspace or use their own devices to go 'online' and enter cyberspace. Law covers the rules of conduct that have been accepted by the government, and which are in force over a certain region, and which must be followed by all people on that region. Breach of these rules could lead to government action such as captivity or fine or an order to pay compensation. Cyber law encompasses laws relating to Cyber Crimes, Electronic and Digital Signatures, Intellectual Property, and Data Protection and Privacy.

Requirement of Cyber Law

There are many grounds why it is difficult for conventional law to manage with cyberspace. The first reason is that Cyberspace is an intangible dimension that is unfeasible to govern and regulate using conventional law. Secondly, cyberspace has complete disregard for jurisdictional boundaries. Another reason is that cyberspace handles huge 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. Cyberspace is absolutely open to sharing by all. Cyberspace offers enormous potential for secrecy to its members. Readily available encryption software and steganographic tools that flawlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens. Electronic information has become the main aim of cyber-crime. It is considered 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 within seconds. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release. Theft of corporeal information such as books, papers, CD ROMs, floppy disks is easily covered by conventional penal provisions. Nevertheless, the difficulty begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities.

In digital world, most of the areas are affected by cyber law. Approximately all transactions in shares are in demat form. All companies comprehensively depend upon their computer networks and keep their valuable data in electronic form. Government forms including income tax returns, company law forms are filled in electronic form. Consumers are progressively more 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. Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography are very common. Digital signatures and e-contracts have reinstated usual methods of transacting business.

To control cyber-crime, Electronic signatures are used to validate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures. Intellectual property refers to the creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law. These include copyright law in relation to computer software, computer source code,

websites, cell phone content, software and source code licences, trademark law with relation to domain names, meta tags, mirroring, framing, linking, semiconductor law which relates to the guard of semiconductor integrated circuits design and layouts, patent law in relation to computer hardware and software. Data protection and privacy laws intend to accomplish a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, and email service providers. These laws try to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Cyber law is new stream for study of law and is increasing at rapid rate. It is vital that user must be aware of basic building blocks of cyber laws, namely Netizens, Cyberspace, and Technology.

Netizens: Cyber law has initiated notion of netizens. A Netizen is an occupant of the worldwide world. He is the one, who inhabits the Net and uses it as an extension of his day-to-day physical world. He reproduces his physical world actions, such as socializing, buying, and selling through online medium. He goes beyond geographical space and time by a click. He identifies no man-made or geographical boundaries. Netizen could be nameless, nameless and faceless person, if he wants to and yet can indulge in various internet activities.

Cyberspace: Cyber laws are made for cyberspace. Cyberspace incorporates the activities, which have occurred in the physical space just prior to entry into cyberspace. Cyberspace is the significant aspect of cyber law which serves as a link between the physical space and the cyberspace, in order to control interface between man and machine. The presence of cyber laws are an expansion of physical laws in cyberspace. These are 'analogy-seeking' laws.

Technology: Cyber laws are devised according to technology used. They turn around technology and its applications. Cyber laws set up norms of acknowledged human behaviour in cyberspace. Currently, there are two-technology school of laws which include technology Specific School and Technology Neutral School. Technology Specific School states that the law should identify only one given set of technology or technology standard. That is, law treats other standards as unlawful, non-binding and thus not allowable. This School offers a single technology platform for the whole community but it disrupts the process of technological innovations and helps in creating monopolistic business. In Indian condition, people follow a technology specific rule. Under the law (The Information Technology Act, 2000), digital signatures using prescribed asymmetric cryptosystem standard is considered legally valid. Use of any other standards would be digital signature unacceptable. When this Act is introduced, the technology procedure was quite low, but with time technology maturity has increased in India and the new Information Technology (Amendment) Bill, 2006 advocate migration towards the technology neutral rule.

The following Act, Rules and Regulations are included under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

Major objectives of the Information Technology Act, 2000 are to provide legal recognition for transactions carried out by means of electronic communication, which is termed as "electronic commerce" and involve the use of alternatives to paper-based methods of communication and

storage of information, to facilitate electronic filing of documents with the Government agencies. The aims of the Act make it a facilitating Act, an enabling Act, and a regulating Act. The Information Technology Act, 2000 is a facilitating Act because it allows both e-commerce and e-governance. The Information Technology Act, 2000 is also considered as an enabling Act which allows legal systems of electronic records and digital signatures.

Though the Internet does not have any geographical limits of a country, one of the United Nations agencies 'United Nations Commission on International Trade Law' (UNCITRAL) recommended a certain level of consistency of laws in all member nations. For this, the Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law (UNCITRAL) to control cyber-crime around the world.

Scope of Cyber Laws

Cyber laws have a broad scope in the current complex situation and eruption of cyber-crime. These laws cover other areas of law having a technology component. Laws related to e-commerce, online contracts, copyright, trademark, business software patenting, e-taxation, e-governance and cyber-crimes fall within the meaning and scope of cyber laws.

To summarize, cyber laws offer the vital mechanism to impeach any person, who is realistically suspected of having committed or of committing or of being about to carry out any offence using any computer, computer system or computer network. Cyber law is an important field of law which represents all the legal issues linked with the internet, and governs all the aspects of the internet and cyberspace, along with dealing in legal cases regarding software patents, net banking and others. Cyber legal representatives perform regular investigations on the major cyber-crimes that are widespread across the internet. With the growing increase in cyber-crimes against individuals, organizations and the government via the internet today, there is a need for strict cyber laws in the global society. Cyber laws which battle cyber-crimes have a dominant effect on any other laws for the time being in force. In India, it was observed that there is a drastic increase in the number of cyber-crimes; therefore, the field of cyber law in India is gaining huge recognition.