CHAPTER 5

Cyber Laws, Safety and Security in India

Contents

Learning Outcomes

After the completion of this chapter, the students will be able to:

- Define Cyber Space and list its features
- Analyse the importance of Cyber Security and Safety
- Explain the meaning of Cyber-crime and the need for Cyber Laws
- Evaluate Cyber Laws in India
- Explain types of Cyber-crimes
- Analyse Cyber-crime and Cyber bullying
- Critically analyse the judicial pronouncement repeating Section 66A of the Information Technology Act, 2000

I. Introduction

We live in a world where we see rapid technological advances on a day-to-day basis. The emergence of advanced digital innovations are providing new opportunities for people from all over the world to connect and communicate. All these opportunities and advances are possible because of the internet. The Internet is defined as, *'a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect'.*

This computer-generated world of the internet that involves interactions between people, software and

services is known as cyberspace. It is a dynamic, exponential and undefined space. As information and the Internet become more complex and large, it has become critical to maintain systems up and running all the time for safety and security.

II. Why do we need Cyber Laws?

When internet was developed, the founding fathers hardly had any idea that it could transform itself into an all pervading revolution which could be misused for criminal activities. Internet usage has significantly increased over the past few years.

The anonymous nature of the internet makes it possible for it to be used for many criminal activities. Cyber Law is important because it touches almost all aspects of transactions and activities on the internet. Every action and every reaction in the cyber space has cyber legal perspectives. Cyber law concerns every individual using the internet like booking a domain name, disputes relating to online intellectual property etc.

III. What is Cyber law?

Cyber law deals with legal issues related to use of inter-networked information technology. It provides the legal rights and restrictions governing technology. In short, cyber law is the law governing computers and the internet.

Cyber law encompasses laws relating to Cyber crimes, Electronic and digital signatures Intellectual property, Data protection and privacy etc.

The Internet was initially developed as a research and information sharing tool and was unregulated. 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.

IV. What is Cyber safety and security?

Cyber safety is the safe and responsible use of information and communication technology.

It is not only about keeping information safe and secure, but also about being responsible with that information and being respectful of other people online. Cyber safety and security can be ensured by enacting laws, and use of technologies, processes and practices that are designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

V. What is Cyber-crime?

Cyber-crime refers to an activity done with criminal intent in cyberspace. In other words, any offence or crime in which a computer is used is a cyber-crime. Even a petty offence like stealing can be brought within the broader purview of cyber crime if the basic data or aid to such an offence is a computer or information stored in a computer used (or misused) by the fraudster. Cyber crimes can be against persons, property or government. For example, cyber stalking, computer vandalism, stealing of data, hacking, phishing, mail fraud etc. The term cyber-crime is not defined in Information Technology Act, 2000 neither in the National Cyber Security Policy 2013 nor in any other regulation in India.

However, 'Cybercrime' has been defined by the National Cyber-crime Reporting Portal (a body set up by the government to facilitate reporting of cyber-crime complaints) to 'mean any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime'.

VI. Categories of Cyber-crime

Cyber-crimes can be divided into three major categories:

1. **Cyber Crime against person-** It includes crimes like cyber stalking, cyber harassment, transmission of child pornography etc.
2. **Cyber Crime against property-** It includes computer trespassing, vandalism and unauthorised possession of computerised information etc.
3. **Cyber Crime against Government-** Cyber terrorism is a distinct kind of crime in this category.
4. **Cyber Harrassment-** Various kinds of harassment can occur in cyber space or by use of cyber space. It can be sexual, racial, religious or others. It can also take within its ambit violation of privacy of netizens (online citizens). Internet makes it easy to invade the privacy of any person which can result in harassment.
5. **Cyber Bullying-** Cyber Bullying is bullying with the help of cyber space and use of devices like cell phone, tablets, laptops etc.

   It can occur through SMS, email, social forums as well as gaming. It means sending, sharing or posting false, derogatory, harmful or negative content about any person. It includes sharing personal information about a person without his or her consent causing humiliation. Cyber bullying can even result in unlawful or criminal behaviour online.

Cyber Bullying and online gaming

Playing video games is a popular past time for children these days. It therefore becomes a platform for cyber bullying. If someone doesn't perform well in a game, he or she becomes a victim of negative remarks and even excluded from the game altogether. This results in cyber bullying.

Sometimes, the bully may use the game as a medium to obtain personal information of the gamers, thereby compromising not just the child's information but also their parents. This tactic is known as Doxing, and makes children more vulnerable to harassment by the bully.

Hacking as a cyber-crime

It is one of the gravest cyber-crimes known. It happens when a stranger breaks into a person's computer system without that person's knowledge or consent and tampers with confidential information. Hacking into government or military owned website results in Cyber Terrorism.

Attack on World Trade Centre- The September 11, 2001 attack on the Pentagon and the World Trade Centre, USA demonstrated the use of cyber space for terrorism. The terrorists gained access to intellectual resources of the government and used it as weapons of destruction. The terrorists hijacked the flight procedures and schedules and executed the ghastly September 11 attack.

Cybersecurity

Under the Act, 'cybersecurity' means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

VII. Cyber Law in India

In India, cyber laws are contained in the Information Technology Act, 2000 which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce and to facilitate filing of electronic records with the Government.

History of Cyber Law in India

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce to bring uniformity in the law in different countries.

The Model Law on Electronic Commerce aims to enable and facilitate commerce conducted by electronic means by providing countries with a set of universally acceptable rules that are aimed at removing legal obstacles and increasing legal predictability for electronic commerce. This model law provides for equal treatment which is essential for enabling paperless communication and fostering efficiency in international trade.

India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

VIII. Scope or Extent of The Information Technology Act, 2000

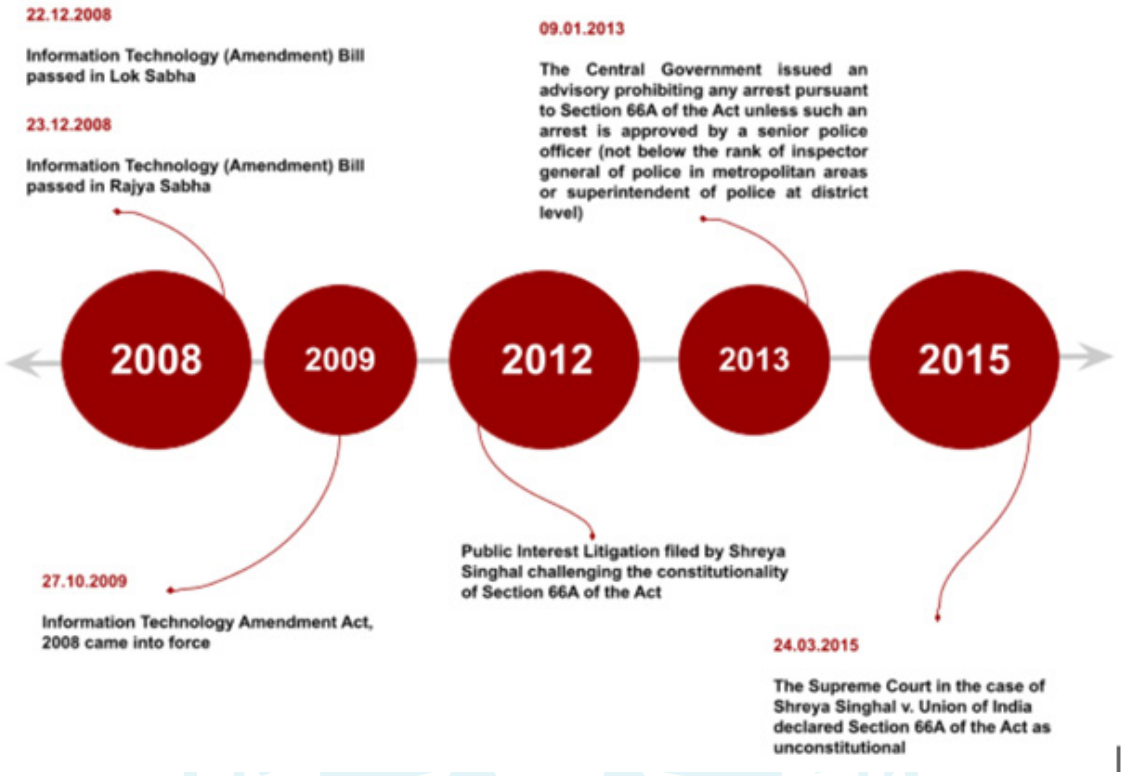
The Information Technology Act, 2000 extends to the whole of India. It also applies to any offence or contravention committed outside India by any person irrespective of his/her nationality, provided such offence or contravention involves a computer, computer system or network located in India.

The courts in India have also recognised cybercrime (eg, the Gujarat High Court in the case of *Jaydeep Vrujlal Depani v State of Gujarat R/SCR.A/5708/2018 Order*), to mean 'the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)'.

The Act provides legal infrastructure for e-commerce, electronic records (like online contracts) and other activities carried out by electronic means. It also deals with electronic governance and cyber crimes.

Interesting Fact : The Information Technology Act, 2000 defines Digital Signature as Authentication of any electronic record by a subscriber by means of electronic method or procedure.

SECTION 66A AND SHREYA SINGHAL



IX. What was Section 66 A IT Act, 2000?

Section 66 A of the IT ACT, 2000 made it a punishable offence for any person to send 'grossly offensive' or 'menacing information' using a computer resource or communication device.

Section 66A was inserted by way of an amendment in the year 2009. The reason behind the amendment was to address new forms of cyber crimes such as publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. Therefore, the said Section 66 A IT Act, 2000 imposed punishment and criminalised the sending of offensive messages through a computer or other communication devices. However, the act used wide terms in this Section which were not defined under the Act and hence caused a lot of confusion as the perception of an individual in defining "grossly offensive" and "menacing information" varies from one individual to another.

In the year 2012, in the matter of Shreya Singhal v. Union of India, a batch of writ petitions were filed under Article 32 of the Constitution of India raising an important question relating primarily to the fundamental right of free speech and expression guaranteed by Article 19 of the Constitution of India. The immediate cause for concern in these petitions was Section 66A of the Information Technology Act of 2000. The petitioners argued that wordings of the section were too wide and ambiguous leading to misuse. Most of the terms used in the section had not been specifically defined under the Act. Further, the petitioners argued that the section restricted the right to free speech and expression prescribed under Article 19(1)(a) of the Constitution of India.

What did the Supreme Court decide?

On March 24, 2015, the Hon'ble Supreme Court struck down Section 66 A of the IT Act, 2000 and declared it unconstitutional for "being violative of Article 19(1)(a) of the Constitution of India.

Interesting Fact : Phishing- The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. (Source: Oxford Dictionary)

X. Exercises

Based on your understanding, answer the following questions:

Q-1 Answer the following questions briefly-

1. Explain the importance of cyber laws in current times.
2. What are the various categories of cyber crime? Give examples.
3. What is cyber bullying? How does it take place?

Q-2 Answer the following questions in about 150 words-

1. Trace the evolution of cyber laws in India.
2. Critically analyse the importance of Section 66A of the Information Technology Act, 2000.

Activities

Q-1 Divide the class into four groups and initiate a discussion on 'Legal problems that arise by use of Cyberspace'.

Q-2 Students can enact a street play making their peers aware of Cyber crime and safety.

Q-3 Debate on the topic 'Cyberspace- A Boon or a bane'.