# UNIT 11 CYBER LAW

**Structure**



## 11.0 INTRODUCTION

In the era of rapid use of information communication technologies networks, devices and services worldwide, the cyberspace has emerged as a new medium of communication. According to International Telecommunication Union (ITU), International Internet bandwidth is growing rapidly worldwide and India is among the front runner nations of the world. In India Internet is growing at a fast pace in cities as well as villages. More and more people are using mobile telephones and this has further accelerated its growth in the country. The new virtual space has thus given rise to many social and national issues and has posed new challenges to deal with technology driven cyber crimes and to protect person's privacy and intellectual rights.

This Unit provides you an overview of the concept of cyber space, cybercrimes and other issues emerging from it.

## 11.1 LEARNING OUTCOMES

After studying this unit you should be able to:

- discuss the concept of cyberspace;
- explain the need for regulation of cyberspace;
- outline various issues emerged due to cyberspace;

- describe cyber crimes and offences under Information Technology (IT) Act; and
- acquaint yourself with the law regulating cyberspace in India.

## 11.2 CONCEPT OF CYBER SPACE

Cyberspace represents a space created by science where various events, sharing of ideas are taking place with the help of Internet connecting various computer systems and mobile phones.

With the advent and growth of electronic communication, the word "cyberspace" has entered into our everyday parlance. But what does this word signify? To a common person, cyberspace refers to a virtual area without limits where one can meet people and discover information on any subject through Internet. In the cyberspace you can find right, wrong or confusing answer to almost any question. This description of cyberspace is not 100% accurate, but it points out some of its important characteristics: its non-physicality, its social dimension and its functionality.

According to Rebecca Bryant, Cyberspace represents "the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication. It appears, then, that space and cyberspace can count as roughly equivalent conceptual entities, at least in the sense of sharing the four common sub-concepts of place: distance, size, time and route.

Despite the differences, cyberspace is, in one way, intimately connected with the physical world. Cyberspace depends, for its very existence, on hardware and software, cables and routers — it depends on physical objects existing in physical space. And, of course, this intimate connection between the two also represents a fundamental difference - physical space, if it exists, depends on nothing at all".

### 11.2.1 Characteristics of Cyberspace

David B. Whittle in his book, "Cyberspace: The Human Dimension", has identified three characteristics of the cyberspace: (1) It is not a physical location but a virtual space. (2) One needs access device to enter into cyber space. That means one needs some sort of physical access device (may be computer screen, a telephone, a terminal, etc.) with an artificial processing mechanism, such as digital computing power and/or software. And that should be joined with other access devices on a network of physical connections.(3) It enables interaction and communication between individuals and groups of individuals and their creative output, largely independent of time and space.

### 11.2.2 Issues emerging from cyberspace and need for regulation

Today new communication technologies, usage of mobile phones and other communication devices are globally challenging the traditional notion of jurisdiction. It has led to the possibility of invasion of the privacy of an individual. There is need to have effective law to deal with the problems of cyber social media crimes, rumour-mongering, email spoofing, spams, cyber stalking, defamation and various other cybercrimes as the impact of these crimes can be more than the conventional crimes. These cyber crimes are usually committed by the person using fake identity, not readily and easily identifiable.

Further, due to anonymity and the ease of circulation it has given rise to many social debates that demands the reconciliation of the two views viz., freedom of speech and expression and the concern for maintaining basic civic peace and standards. Besides this, the major areas of concern which calls for strict regulation are: Management of Intellectual Property and to prevent Infringements in digital media; spread of terrorism, cross border taxation; cyber security which is an expensive affair as the business organisations are vulnerable to data breaches leading to loss of business opportunities and therefore needed to be secured from unauthorised access, modification or removal of data/information, data theft; authentication, data protection and data privacy of the industries, individuals and government agencies; Encryption; Protection of e-consumers from the misleading advertisements of goods and services enabling them to make informed and meaningful choices. The business organisations must manage the consumer information responsibly respecting the privacy of the individuals but this requires strict regulators restricting the exchange and use of data.

**Check Your Progress: 1**

**Note:** 1) Use the space below for you answers.

2) Compare your answers with those given at the end of this unit.

1) What are the characteristics of cyber space?

.....

.....

.....

.....

.....

.....

2) Why do we need cyberspace regulation?

.....

.....

.....

.....

.....

## 11.3 INTERNATIONAL AND NATIONAL CYBER LAWS

In this section we shall briefly discuss the international and national laws which govern cyberspace.

### 11.3.1 International Law

UNCITRAL Model law 1996, Model law on E-Signature, 2001 and United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 constitute some international initiatives relating to cyberspace.

**UNCITRAL Model law 1996 -**The first Model Law on E-commerce was adopted in 1996 by United Nations Commission on International Trade and Law (UNCITRAL). The General Assembly of United Nations adopted it by passing a resolution on 30th January, 1997. The prime objective of the law was to have uniformity in law relating to e-commerce at international level and to provide equal treatment to paper-based and electronic information. India is also signatory to this Model law and hence, enacted the Information Technology Act, 2000.

**Model law on E-Signature, 2001(MLES)** - In 2001, the Model law on E-Signature was adopted by United Nations Commission on International Trade and Law (UNCITRAL) with the aim to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. The law may assist countries in establishing a modern, harmonised and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status. Accordingly, India passed the Information Technology (Amendment) Act, 2008, which makes necessary amendments in 2000.

United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 - It was adopted in 23 November 2005 and came into force on 1 March 2013. It recognises the fact that electronic communications plays a fundamental role in promoting trade and economic development both domestically and internationally and also improves the efficiency of commercial activities. It aims to provide a common solution to remove legal obstacles to the use of electronic communications in a manner acceptable to States with different legal, social and economic systems. The Electronic Communications Convention aims at facilitating the use of electronic communications in international trade by assuring that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents.

## 11.3.2 National Law

The Government of India being signatory to UNICITRAL LAW on E-commerce enacted the 2000 which was amended in the year 2008 to implement the UNCITRAL Model Law on Electronic Signatures, 2001. Many traditional crimes which are capable of being committed with the use or aid of or through computers and technology have been bought within the definition of conventional crimes and therefore fall under the ambit of the Indian Penal Code, 1860 as amended. The Evidence Act, 1872 has been amended, section 65A and section 65B of the Indian Evidence Act, 1872 provides for Admissibility of electronic records as evidence. The Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, have also been amended in order to facilitate collection of evidence to deal with cyber crimes or any matter connected with such crimes. The main purpose of these amendments is to address the related issues of electronic commerce, electronic crimes and evidence and to enable further regulation with regard to Electronic Fund Transfer.

For further detailed information, you may visit website of United Nations Commission on International Trade Law: www.unicitral.org.

## 11.4 INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 aims to provide legal recognition for the transactions carried out by the means of electronic data interchange and other means of communications commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper based methods of the communication and storage of information, to facilitate electronic filing of document with the government agencies.

### 11.4.1 Electronic signature and Electronic records

Section 3A of the Information Technology Act provides that a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which (*a*) is considered reliable; and (*b*) may be specified in the Second Schedule.

Chapter III of the Act pertains to legal recognition to the electronic records (Section 4), electronic signature (Section 5) and their usage in Government and its agencies (Section 6). Chapter IV lays down rules for attribution of the e-record, the mode and manner of its acknowledgement and determination of time and place of dispatch and receipt of electronic records. Section 10A provides for validity of contracts formed through electronic means. Chapter V lays down conditions for secure electronic records and secure electronic signature.

### 11.4.2 Regulation of Certifying Authorities

The provisions relating to Regulation of Certification Authorities are given in Chapter VI of the Information Technology Act. Chapter VI deals with appointment of a controller and other officers, functions of controller, recognition of foreign certifying authorities, licence to issue electronic signature certificates – application, renewal, suspension of licence and procedure for grant or rejection of licence.

**Functions of Controller**

Controller of Certification authority is a focal point in the Information Technology Act, who shall discharge the functions under this Act subject to the general control and directions of the Central Government. According to Section 18 of the Information Technology Act, the Controller may perform all or any of the following functions:

a) Exercising supervision over the activities of the Certifying Authorities.

b) Certifying public keys of the Certifying Authorities.

c) Laying down the standards to be maintained by the Certifying Authorities.

d) Specifying the qualifications and experience which employees of the Certifying Authorities should possess.

e) Specifying the conditions subject to which the Certifying Authorities shall conduct their business.

f) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key.

g) Specifying the form and content of a Digital Signature Certificate and the key.

h) Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities.

i) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.

j) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems.

k) Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.

l) Resolving any conflict of interests between the Certifying Authorities and the subscribers.

m) Laying down the duties of the Certifying Authorities.

n) Maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

**Powers of Controller**

In Section 24 of the procedure for grant or rejection of licence is stated. According to this Section, the Controller may, on receipt of an application under Section 21(1), and after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application. However, no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

In Section 25 of the procedure for suspension of licence is laid down. According to this Section:

1) the Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has-

   a) made a statement that the application for the issue or renewal of the licence is incorrect or false in material particulars;

   b) failed to comply with the terms and conditions subject to which the licence was granted;

   c) failed to maintain the procedures and standards specified in Section 30;

   d) contravened any provisions of this Act, its rules, regulations or orders; revoke the licence: Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under the above sub-section (1), by order, suspend such liecnce pending the completion of any enquiry ordered by him. However, no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

Sections 28 and 29 of the Act provide power to the Controller or any officer authorised by him to investigate contraventions and to access to computers and data if he has reasonable cause to suspect any contravention of the provisions of this Act, its rules or regulations.

### 11.4.3 Cyber Appellate Tribunal

Section 57 of Information Technology Act lays down provisions relating to Appeal to Cyber Appellate Tribunal.

- Any person aggrieved by an order made by controller or an adjudicating officer under this Act may file an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter, within forty-five days of receipt of the copy of the said order. However, no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. The Cyber Appellate Tribunal can also entertain an appeal after the expiry of the said period of forty-five days, if it is satisfied that there was sufficient cause for not filing it within that period.

- The Cyber Appellate Tribunal shall give both the parties to the appeal, an opportunity of being heard before passing such orders.

- The appeal filed before the Cyber Appellate Tribunal shall be disposed off as expeditiously as possible with an endeavor for final dispose within six months from the date of receipt of the appeal.

**Procedure and powers of the Cyber Appellate Tribunal**– Section 58 of Information Technology Act provides that the Cyber Appellate Tribunal has, for the purposes of discharging its functions, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying the suit. However, the Tribunal shall not be bound by the procedure laid down by Section 5 of Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this Information Technology Act and its rules. The Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

### 11.4.4 Intermediaries

Section 2(1) (w) of Information Technology Act defines: Intermediary means any person who on behalf of another person receives stores or transmits that record or provides any service with respect to that record. Intermediary includes: telecom service providers; network service providers; internet service providers; web-hosting service providers; search engines; online payment sites; online-auction sites; online-market places and cyber cafes.

As the Internet has grown to permeate all aspects of the countries and economy; the role of Internet intermediaries in bringing together or facilitating interactions, transactions or activities between third parties on the Internet is crucial as they influence and determine access to and choice between online information, services and goods.

**Duties of Intermediaries**:

- According to Section 67 C of Information Technology Act, Intermediary shall preserve and retain such information as may be specified for such

duration and in such manner and format as the Central Government may prescribe. In case of intentionally contravening this duty, the Act provides that intermediary shall be punished with an imprisonment for a term, which may extend to three years and also be liable to fine.

- Section 69(3) provides that the subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, must extend all facilities and technical assistance them. Intermediary will provide them access to (a) the computer resource generating, transmitting, receiving or storing such information; or (*b*) intercept, monitor, or decrypt the information; or (*c*) information stored in computer resource.

- Information Technology Act also deals with blocking public access of any information through any computer resource. The intermediary has to comply with the direction issued by the Government in this regard. In case, the intermediary fails to comply with the direction issued shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

**Role of intermediaries and the law**

Intermediaries play an important role and act as the tools that enable users to access information and provide new opportunities for social activities and citizen participation. Their technical capacity to prevent harm by strengthening cyber security, e-consumer security and to protecting privacy and intellectual property rights are very important. It has always been the concern across the world that besides certain duties and responsibilities the intermediaries must also be given protection or exemption from legal liability that could arise due to posting of illegal content by the users. In many countries like the USA and members of the European Union, there are attempts to provide legal protection to intermediaries from such user generated content. Such protection is often termed as a 'safe harbour' protection. Our Information Technology Act also provides for exemption from liability of intermediary in certain cases as discussed below:

**Exemption from liability**

Under Information Technology Act intermediaries are not liable for any third party information, data, or communication link made available to others in following cases:

*a*) Where the intermediary does not–

  *i*) initiate the transmission,

  *ii*) select the receiver of the transmission, and

  *iii*) select or modify the information contained in the transmission;

b) Where the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe from time to time.

**Liability of intermediaries**

Intermediary will be liable in the following circumstances:

a) Where the intermediary has conspired or abetted whether by threats or promise or otherwise in the commission of the unlawful act;

b) On being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, if the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

**Check Your Progress: 2**

**Note:** 1) Use the space below for you answers.

2) Compare your answers with those given at the end of this unit.

1) Define the term 'intermediaries'.

.....

.....

.....

.....

.....

.....

2) Who can file an appeal to Cyber Appellate Tribunal?

.....

.....

.....

.....

.....

.....

## 11.5 CYBER CRIMES

The term cyber crime refers to the wide range of crimes that involves computers and networks, where computer is used as a tool to commit crime or computer itself is the target of a crime or incidental to a crime. The term cyber crimes, if used in generic sense, its scope can be extended to covers many kinds of civil and criminal wrongs**.** The cyber crimes are committed against individuals or property, they are also committed against an organisation - Government, non government; company; firm or group of individuals, or against the society at large.

### 11.5.1 Types of Computer Crimes

Computer crimes can be categorised as given below:

**Conventional crimes committed through computer**: There are a number of traditional or conventional crimes that are committed against individuals and

their properties. Many of these crimes are now being committed by the aid of computers. Cyber defamation, cyber pornography, cyber stalking/harassment, cheating, digital forgery, theft, Internet fraud/ financial crimes including cheating, credit card frauds, money laundering online gambling and sale of illegal articles, cyber terrorism etc are the crimes punishable under both Indian Penal Code and Information Technology Act.

Cyber defamation (publication of defamatory statement about someone on a website or sending of e-mails containing defamatory information to the known contacts of the victim) is covered under section 499 of Indian Penal Code (IPC) read with section 4 of the Information Technology Act. Cyber frauds are also covered under Section 420 IPC. Digital forgery of documents is creation of a document which one knows is not genuine and yet projects the same as if it is genuine. Fraudulent birth certificates, ID cards, etc are dealt with various sections of IPC and Information Technology Act. Cyber stalking, i.e. repeated acts of harassment or threatening behaviour of the criminal targeting the victim with the aid of the Internet, e-mail, or other electronic communication devices to stalk another person, is a cybercrime as well as a crime under IPC. Cyber pornography, showing of sexual acts can be dealt with under Sections 292 and 293 IPC, Sections 67,67A and 67B Information Technology Act and Indecent Representation of Women's Act.

**Crimes committed on a computer network and related to mail**: These crimes are technology driven crimes like hacking/unauthorised access, E-mail spamming, or E-mail spoofing. E-mail spamming mans an illegal intrusion into a computer system and/or network. E-mail spamming also means sending of large amount of mails to the victims as a result of which their account or mail server crashes. Email spoofing means an e-mail that appears to originate from one source although it has actually been sent from another source. These crimes are dealt with under Indian Penal Code as well as Information Technology Act.

**Crimes relating to data alteration/destruction**: computer vandalism, transmitting of virus/worms/Trojan horses/ logic bomb, theft of Internet hours; data diddling, salami attacks- insignificant alteration in customers account which in a single case would go completely unnoticed; phishing, etc. Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system, most often by a data entry clerk or a computer virus. Phishing is a sort of cyber crime often used to steal user data, including login credentials and credit card numbers, etc. Usually it is committed by a person under the disguise of some trustworthy entity.

Section 43 of Information Technology Act also provides for civil liability.

**Crimes relating to violation of Intellectual property rights**- The examples are distribution of pirated software; and cyber squatting i.e., obtaining of a domain name consisting of the owner's distinctive trademark. The traditional laws for protecting intellectual property have also been applicable to the infringements taking place in digital media.

### 11.5.2 Cyber Crimes: Some Cases

It will be useful for you to know about some cases related to cyber crimes dealing with fake identity, defamation, cheating, and cyber pornography, publishing or transmitting obscene material in electronic form, etc.

**SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, decided by ADJ, Delhi on 12 February 2014**

In this case it was alleged that defendant Jogesh Kwatra being an employee of the plaintiff company had sent derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The plaintiff filed a suit for permanent injunction restraining the defendant from doing the above said illegal acts. The Hon'ble Judge of the Delhi High Court passed an ex-parte interim injunction observing that a prima facie case had been made out by the plaintiff and consequently restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. The defendant was further restrained from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

However ADJ, Delhi in the judgment dated 12 February 2014 held that "this court is not in a position to accept the strongest argument on behalf of plaintiff under the circumstances in the absence of direct evidence to infer that it was the defendant in particular, who was sending these emails - the test of balance of probabilities is to be applied to the evidence available on record and not to the inferences". The issue was accordingly decided against the plaintiffs and in favour of the defendant and suit of the plaintiff was dismissed.

**State of Tamil Nadu Vs Suhas Katti**, **AMM Court, Egmore (CC No 4680 of 2004)**

This is considered as the first case in India of conviction under Section 67 of 2000. In this case the accused, a known family friend of the victim was interested in marrying her. However, the victim married another person and that marriage later ended in divorce. The accused started contacting her once again but she turned down his marriage proposal. The accused took up harassment of the victim through the Internet by posting obscene, defamatory and annoying message about her in the yahoo message group and then forwarding emails to the victim through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in messages and phone calls from several persons to the victim who also received phone calls by people who believed she was soliciting for sex work.

The accused was found guilty and sentenced for offences under section 67 of Information Technology Act 2000 and 469, 509 of the IPC. The sentence included imprisonment for two years and fine.

**National Association Of Software** (NASSCOM), **vs Ajay Sood and Others,** Decided by Delhi High Court on 23 March 2005.

In this case the defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of NASSCOM. Plaintiff filed the suit praying for a decree of permanent injunction restraining the defendants or any person acting under their

authority from circulating fraudulent E-mails purportedly originating from the plaintiff of using the trade mark 'NASSCOM' or any other mark confusingly similar in relation to goods or services. Prayer for damages was made in the plaint.

This landmark judgment delivered on 23rd March 2005 brings the act of **"phishing**" into the ambit of Indian laws even in the absence of specific legislation. The court observed that "An act which amounts to phishing, under the Indian law would be a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even the person whose name, identity or password is misused. It would also be an act of passing off as is affecting or tarnishing the image of the plaintiff, if an action is brought by the aggrieved party."

The defendants in the present case admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks. Defendants their servants and agents were barred from circulating fraudulent e-mails purportedly originating from the plaintiff or using the trade name NASSCOM or any other name/mark and address of the plaintiff amounting to tarnishing their image.

**Activity-1**

Go through newspaper reports and identify some cyber crimes dealing with fake identity, defamation, cheating, etc. as discussed above. Follow up the stories and analyse the outcome.

**Check Your Progress: 3**

**Note:** 1) Use the space below for you answers.

2) Compare your answers with those given at the end of this unit.

1) Explain the term 'phishing'.

.....

.....

.....

.....

.....

2) What is Data Diddling?

.....

.....

.....

.....

## 11.6 LET US SUM UP

In this unit we discussed various aspects relating to Cyber law such as the concept of cyberspace; the need for regulation of cyberspace; cyber crimes and offences under Information Technology (IT) Act; and the law regulating cyberspace in India.

Today cyberspace has emerged as a new medium of communication, a place where numbers of social and economic activities are going on leading to new challenges and new forms of crimes. Some of these involve computers and networks, where computer may be used as a tool to commit crime or computer itself is the target or computer may be considered as incidental to a crime. Therefore the role of internet intermediaries, their technical capacity to prevent harm by strengthening cyber security, e-consumer security and in protecting privacy and intellectual property rights cannot be denied. It was discussed that the intermediaries need to observe due diligence while discharging their duties. The applicable law to govern electronic records and technology driven crimes is Information Technology Act, 2000. It was also explained that many traditional crimes which are capable of being committed with the use or aid of or through computers and technology can also be dealt with under Indian Penal Code, 1860; The Evidence Act, 1872, The Banker's Book Evidence Act, 1891and and the Reserve Bank of India Act, 1934, and others.

## 11.7 FURTHER READINGS

Gibson, William, *Neuromancer*, Harper Collins Publishers, London, 1995, p.67 S. SAI

Pavan Duggal, Cyber Law, Universal Law Publishing Co., Delhi, Second Edition, 2017

Prashant Mali, *Cyber law & cyber crimes simplified*, Cyber Infomedia, 4th edition. 2017

Vakul Sharma, *Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce*. Universal Law Publishing - An imprint of Lexis Nexis. 5th edition. 2016

Dr.S.R. Myneni**,** *Information Technology Law (Cyber Laws)*, Asia Law House, 2017

## 11.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

**Check Your Progress: 1**

1) Cyberspace is not a physical location but a virtual space. One needs access device to enter into cyber space. That means one needs some sort of physical access device (may be computer screen, a telephone, a terminal, etc.) with an artificial processing mechanism, such as digital computing power and/or software. That should be joined with other access devices on a network of physical connections. It enables interaction and communication between

individuals and groups of individuals and their creative output, largely independent of time and space.

2) Today new communication technologies, usage of mobile phones and other communication devices are globally challenging the traditional notion of jurisdiction. This has led to the possibility of the invasion of privacy of an individual. We need effective law to deal with the problems of cyber social media crimes, rumour-mongering, e mail spoofing, spams, cyber stalking, defamation and various other cybercrimes as the impact of these crimes can be more than the conventional crimes. These cyber crimes are usually committed by the person using fake identity thus not readily and easily identifiable.

**Check Your Progress: 2**

1) Section 2(1) (w) of Information Technology Act defines Intermediary any person who on behalf of another person receives stores or transmits that record or provides any service with respect to that record. Intermediary includes: telecom service providers; network service providers; internet service providers; web-hosting service providers; search engines; online payment sites; online-auction sites; online-market places and cyber cafes.

2) Any person aggrieved by an order made by controller or an adjudicating officer can file an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter, within forty-five days of receipt of the copy of the said order. However no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties

**Check Your Progress: 3**

1) Phishing is a sort of cyber crime often used to steal user data, including login credentials and credit card numbers, etc. Usually it is committed by a person under the disguise of some trustworthy entity.

2) Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system, most often by a data entry clerk or a computer virus.