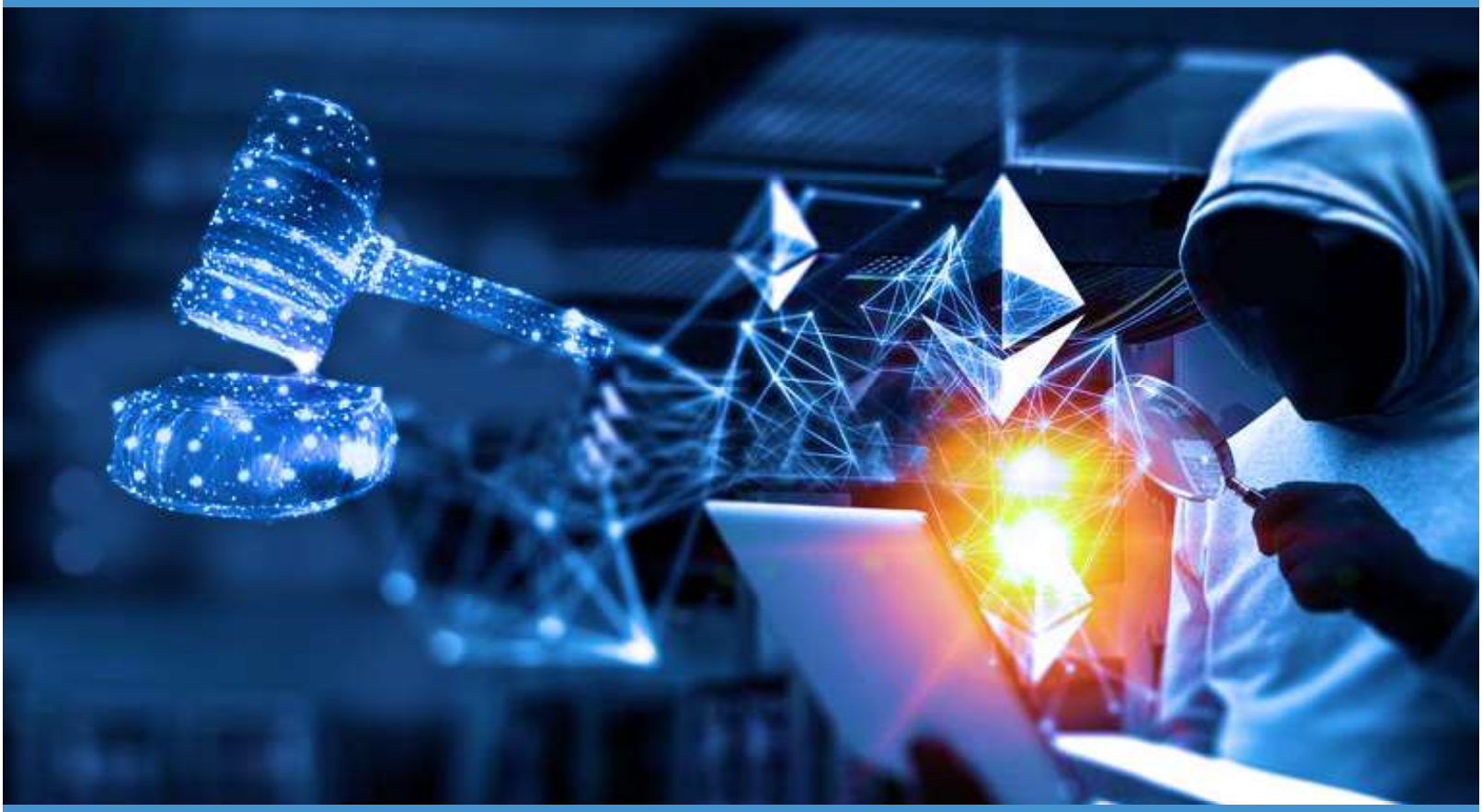
Dr.Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-103

Domestic Regulatory Framework



Post Graduate Diploma in Cyber Law (PGDCL)

2020

Domestic Regulatory Framework

Dr. Babasaheb Ambedkar Open University

Domestic Regulatory Framework

Course Writer

Dr.DeeshaKhaire Assistant Professor (Law), Gujarat National Law University, Gandhinagar

Content Editors

Prof. (Dr.) Nilesh K. Modi Professor & Director, School of Computer Science
Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat

ISBN:978-81-949119-9-9

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

Domestic Regulatory Framework

Block-1: INFORMATIONAL TECHNOLOGY ACT, 2000(AMENDED IN 2008): BRIEF UNDERSTANDING

Block-2: DIGITAL SIGNATURE, ELECTRONIC SIGNATURE AND LAWS RELATED TO CERTIFYING AUTHORITY OF INDIA

Block-3: LAWS RELATED TO E-SERVICE DELIVERY AND SERVICE PROVIDERS

Block-4: LAWS RELATED TO DATA PROTECTION IN INDIA

Block-1
Information Technology Act, 2000 (Amended in 2008): Brief Understanding

Unit 1: Jurisdictional Aspects of Cyber Law

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Issues of Jurisdiction
- Territorial and Extraterritorial Jurisdiction
- Various tests involved to determine jurisdiction

1.2 INTRODUCTION

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Jurisdiction is the authority of a court to hear a case and resolve a dispute involving person, property and subject matter. The principles of jurisdiction are

enshrined in the Constitution of a State and part of its jurisdictional sovereignty.[1] All sovereign independent States possess jurisdiction over all persons and things within its territorial limits and all causes, civil and criminal, arising within these limits.[2]

1.3 ISSUES OF JURISDICTION

The issue of jurisdiction has been looked at from two perspectives.[3] They are:-

- ***Prescriptive Jurisdiction***

  It describes a State's ability to define its own laws in respect of any matter it chooses. A State's prescriptive jurisdiction is unlimited and a State may legislate for any matter irrespective of where it occurs or the nationality of the persons involved.

- ***Enforcement Jurisdiction***

  A State's ability to enforce laws is necessarily dependent on the existence of prescriptive jurisdiction.A State's enforcement jurisdiction within its own territory is presumptively absolute over all matters and persons situated therein. The State's legislative enactments primarily reflect its prescriptive jurisdiction.

1.4 EXTRATERRITORIAL JURISDICTION

Public International Law reflects the juxtaposition of States (as a legal person) and subjects their jurisdictional sovereignties to certain limitations, i.e., there is 'general prohibition in international law against the extraterritorial application of domestic laws.[4] The Supreme Court in ***British India Steam Navigation Co. VsShanmughavilas Cashew Industries***[5]***,*** while dealing with Private International law, however made general observations as to the extent of

[1] Apart from judicial activity, a State's administrative, executive and legislative activity is also part of its jurisdictional sovereignity

[2] Lord Macmillan in Compania*NavieraVascongado v Steamship Cristina*, [1938] AC 485

[3] 'Cyberspace Jurisdiction and Courts in India' by Dr Ravishankar K Mor, Asst Prof Dept of Law,YeshwantMahavidyalaya, Wardha

[4] In the absence of municipal laws, international treaties ratified by India can be taken into account for framing guidelines in respect of enforcement of fundamental rights. (*Vishaka v State of Rajasthan*, [1997] 6 SCC 241, *Lakshmi Kant Pandey v Union of India*, AIR [1984] SC 469

[5]*British India Steam Navigation Co. v Shanmughavilas Cashew Industries* [1990] 48 ELT 481 (SC).

applicability of the statutes enacted by the Indian Parliament and opined: "In general, a statute extends territorially, unless a contrary is stated, throughout the country and will extend to the territorial waters and such places as intention to such places is shown". It was further observed that "without anything more, Indian statutes are ineffective against foreign property and foreigners outside the jurisdiction".

The sources of the extraterritorial jurisdiction are:

a) Territorial Principle

A State's territory for jurisdictional purposes extends to its land and dependent territories, airspace, ships, territorial sea and, for limited purposes to its contiguous zone, continental shelf and Exclusive Economic Zone (EEZ). The said principle as adopted by the national courts has been that all persons within a State's territory are subject to national law, save only for those granted immunity under international law.

The territorial principle has two variants:

a) 'Objective' territorial principle, where a State exercises its jurisdiction over all activities that are completed within its territory, even though some element constituting the crime or civil wrong took place elsewhere; and

b) 'Subjective' territorial principle, where a State asserts its jurisdiction over matters commencing in its territory, even though the final event may have occurred elsewhere.

In ***SS Lotus Case (France Vs Turkey),***[6]it was held by the Permanent Court of International Justice that "the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial i.e., it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".

b) Nationality Principle

It is for each State to determine under its own law who its nationals are. The nationality of a person of a particular State shall be determined in accordance with the law of that State.

[6]*SS Lotus Case (France v Turkey)*PCIJ Ser A [1927], No 9

Nationality serves above all to determine that the person upon whom it is conferred, enjoys the rights and is bound by the obligations which the law of the State in question grants to or imposes upon its nationals.[7]

c) Protective Principle

A State relies upon this principle when its national security or a matter of public interest is in the issue. A State has a right to protect itself from acts of international conspiracies and terrorism, drug trafficking, etc.

In ***Attorney-General of the Government of Israel v Eichmann,***[8] the District Court of Jerusalem held:

The State of Israel's 'right to punish' the accused derives, in our view, from two cumulative sources: a universal source (pertaining to the whole of mankind), which vests the right to prosecute and punish crimes of this order in every State within the family of nations; and a specific or national source, which gives the victim nation the right to try any who assault its existence.

d) Passive Personality Principle

It extends the nationality principle to apply to any crime committed against a national of a State, wherever that national may be. It, in a way, provides that the citizen of one country, while visiting another, takes with him for his "protection" the law of his own country and subjects the operation of that law upon those with whom he comes into contact. The passive personality principle authorizes States to assert jurisdiction over offences committed against their citizens abroad.[9] It recognized that each State has a legitimate interest in protecting the safety of its citizens when they journey outside national boundaries. Though the principle may be referred to as a controversial one, as it extends the ***'arm of national laws further even in the foreign territories'.*** Nevertheless, the principle has been adopted as a basis for asserting jurisdiction over hostage-takers.[10]

e) Universality Principle

[7] *Nottebohm Case (Liechtenstein v Guatemala*) (Second Phase), ICJ Rep [1955] 4
[8] *Attorney-General of the Government of Israel v Eichmann* 36 ILR [1961] 5
[9] *United States v Yunis*, 681 F Supp 896 [1988]
[10] See, International Convention against the taking of hostage, 1979

The canvass of the universality principle is quite vast. A State has jurisdiction to define and prescribe punishment for certain offences recognized by the community of nations as of universal concern. It includes acts of terrorism, attacks on or hijacking of aircrafts, genocide, war crimes etc. A State may assert its universal jurisdiction irrespective of who committed the act and where it occurred.

The principles of jurisdiction of international law take cognizance of both State and international laws. If on one hand the objective of the State (or municipal or domestic) law is not only to ascertain the supremacy of its judicial sovereignty domestically but also extra-territorially, then on the other the international law itself imposes general prohibition against the extraterritorial application of domestic laws.

1.5 THE EFFECTS DOCTRINE

It is an extra-territorial application of national laws where an action by a person with no territorial or national connection with a State has an effect on that State. The situation is compounded if the act is legal in the place where it was performed. The 'Effects Doctrine' is primarily a doctrine to protect American business interests and is applicable where there are restrictive trade or anti-competitive agreements between corporations. In ***Hartford Fire Insurance Co. Vs California***[11]***,*** the question was whether the London Insurance Companies refusing to grant reinsurance to certain US businesses, except on terms agreed amongst themselves are violative of the US anti-trust laws and tried in the United States. The US Supreme Court held that the US Court did have jurisdiction and that there exists no conflict between domestic and foreign law and "where a person subject to regulation by two states can comply with the laws of both".

1.6 PERSONAL JURISDICTION

Personal Jurisdiction is the competence of a court to determine a case against a particular category of persons (natural as well as juridical). It requires a determination of whether or not the person is subject to the court in which the case is filed. It is classified into:-

- ***General Jurisdiction***

[11] *Hartford Fire Insurance Co. v California* 113 S Ct 2891 [1993]

The General Jurisdiction subjects a person to the power of the applicable court with respect to any cause of action that might be brought. It has historically relied on very close contacts of the person with the state, such as residency or domicile within the state, physical presence in the state at the time of service of process, etc.

- ***Specific Jurisdiction***

The Specific Jurisdiction refers to the power of the applicable court with respect to a particular cause of action based upon some set of 'minimum contacts' with the forum state that relate to that cause of action.

1.7 TESTS INVOLVED TO DETERMINE JURISDICTION

- ***Minimum Contacts Test***

In ***International Shoe Co. Vs Washington***[12]***,*** a two-part test for determining the jurisdiction of the forum court over a defendant not residing or carrying on business within its jurisdiction was evolved. It was held that in such an instance, the plaintiff would have to show that the defendant has sufficient'minimum contacts' in the forum state. In other words, the defendant must have purposefullydirected its activities towards the forum state or otherwise 'purposefully availed' of the privilege of conducting activities in the forum state. Further, the forum court had to be satisfied that exercising jurisdiction would comport with the traditional notions of fair play and substantial justice. The minimum contacts test in the said case has been understood as to have performed "two related, but distinguishable, functions."[13] The first was to protect the defendant from the burden of litigating in a distant or inconvenient forum.[14] The second was to ensure that the states do not "reach out beyond the limits imposed on them by their status as coequal sovereigns in a federal system."[15]

- ***Purposeful Availment Test***

In ***Burger King Corp VsRudzewicz***[16]***,*** the Supreme Court held that the defendant did not have to be physically present within the jurisdiction of the forum court and that the forum court may exercisejurisdiction over a non-resident where an alleged injury arises out of or

[12] *International Shoe Co v Washington* 326 U S 340 [1945]
[13] *World-Wide Volkswagen v Woodson*, 444 U.S. 286, 291-92 [1980]
[14] Id
[15] Supra note 12
[16] *Burger King Corp v Rudzewicz*471 U S 462 [1985]

relates to actions by the defendant himself that are 'purposefully directed' towards residents of the forum state. It was held that **'purposeful availment'** would not result from 'random' or 'fortuitous' contacts by the defendant in the forum state. It requires the plaintiff to show that such contracts resulted from the "actions by the defendant himself that created a substantial connection with the forum state." He must have engaged in 'significant activities' within the forum state or created 'continuing obligations' between himself and the residents of the forum state. It was held on facts, the twenty-year relationship that the defendant had with the plaintiff "reinforced his deliberate affiliation with the forum state and the reasonable foreseeability of litigation there."

In ***Ballard v. Savage***[17]**,**it was explained that the expression 'purposefully availed' meant that "thedefendant has taken deliberate action within the forum state or if he has created continuing
obligations to forum residents." It was further explained that "it was not required that a defendant be physically present within, or have physical contacts with the forum, provided that hisefforts are purposefully directed toward forum residents."

In ***CompuServe, Inc. v. Patterson***[18]**,** it was found that the defendant had chosen to transmit its products from Texas to CompuServe's system and that the system provided access to his software to others to whom he had advertised and sold his product. It was held that Patterson had "purposefully availed himself of the privilege of doing business."

- ***Sliding Scale Test***

An extension of the purposeful availment test was attempted in ***Zippo Mfg. Co. v. Zippo Dot Com,Inc.***[19]The issue of specific personal jurisdiction arose in the context of trademark dilution, infringement and false designation under the Federal Trademark Act. The court in ***Zippo***classified websites as passive, interactive and integral to the defendant's business. It was held that "At one end of the spectrum are situations where a defendant clearly does businessover the Internet. If the defendant enters into contracts with residents of a foreignjurisdiction that involves the knowing and repeated transmission of computer

[17]*Ballard v Savage*65 F3d 1495 (9th Cir) [1995]
[18]*CompuServe, Inc v Patterson*89 F 3d 1257 (6th Cir) [1996]
[19]*Zippo Mfg Co v Zippo Dot Com,Inc*952 F Supp 1119 (W D Pa) [1997]

filesover the Internet, personal jurisdiction is proper. At the opposite end are situationswhere a defendant has simply posted information on an Internet Website, which isaccessible to users in foreign jurisdictions. A passive Website that does little morethan make information available to those who are interested in it is not grounds forthe exercise of personal jurisdiction. The middle ground is occupied by interactiveWebsites where a user can exchange information with the host computer. In thesecases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Website".

In ***Millennium Enterprises Inc. v. Millennium Music L.P.***[20] the Oregon district court declined toexercise jurisdiction over a South Carolina corporation that sold products both offline and on the web. The court felt that ***'something more'*** than merely showing that the website was interactive was required. The defendant should be shown to have consummated some transaction within Oregon and to have made 'deliberate and repeated contacts' with Oregon through the website so that it could be held that they ought to have anticipated being hauled into an Oregon court.

1.8 THE EFFECTS TEST AND INTENTIONAL TARGETING

The difficulty experienced with the application of the ***Zippo sliding scale test*** has paved the way for the application of the 'effects' test. The courts have thus moved from a 'subjective territoriality' test[21]to an 'objective territoriality' or 'effects' test in which the forum court will exercise jurisdiction if itis shown that effects of the defendant's website are felt in the forum state. In other words, it musthave resulted in some harm or injury to the plaintiff within the territory of the forum state. Sincesome effect of a website is bound to be felt in several jurisdictions given the nature of the internet,courts have adopted a 'tighter' version of the 'effects' test, which is 'intentional targeting.'

[20]*Millennium Enterprises Inc v Millennium Music L P*33 F Supp 2d 907 (D Or) [1999]

[21] That a court will regulate an activity only if it is shown having originated in its territory – exemplified by the decisionin *Louis Feraud Int'l SARL v Viewfinder Inc*,406 F Supp 2d 274 (S D N Y) [2005]

The 'effects' test was first evolved in ***Calder v. Jones.***[22]In the said case, the Court held that a California court could assert jurisdiction over a Florida publisher that published an article defaming the plaintiff, in view of the facts that the plaintiff resided in California. The Court reasoned that the defendants had engaged in "intentional, and allegedly tortious, actions that were expressly aimed at California", and that "they knew that the brunt of the injury would be felt" by the plaintiff in California.

The 'Effects Test' is a further extension of the 'forum state targeting', as it also takes into consideration the effect that "out-of-state" conduct has in the forum state. Thus, in order to have personal jurisdiction, there must be:-

- Intentional actions
- Expressly aimed at the forum state
- Causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state.

1.9 LET'S SUM UP

In this chapter, we have studied the issues of jurisdiction along with extraterritorial and personal jurisdiction. We also studied the tests involved in determining jurisdiction. Finally, we ended the discussion with the Effects Test and Intentional targeting.

1.10 FURTHER READING

- Brenner, Susan. (2004). Cybercrime jurisdiction. J. High Tech. L. 1. 10.1007/s10611-007-9063-7.
- Brenner, Susan &Koops, Bert-Jaap. (2005). Approaches to Cybercrime Jurisdiction. Journal of High Technology Law. 4.
- Egyankosh.ac.in (2019), http://egyankosh.ac.in/bitstream/123456789/7634/1/Unit-10.pdf (last visited Nov 27, 2019).

[22]*Calder v Jones*465 U S 783 [1984]

- AmitaVerma, Cyber Crimes and Law, Central Law Publications, Allahabad, 2009, p.318.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the issues of jurisdiction associated with cyber laws?

The issues of jurisdiction associated with cyber laws are as follows:

- *Prescriptive Jurisdiction* - It describes a State's ability to define its own laws in respect of any matter it chooses. A State's prescriptive jurisdiction is unlimited and a State may legislate for any matter irrespective of where it occurs or the nationality of the persons involved.
- *Enforcement Jurisdiction* – It deals with a State's ability to enforce laws is necessarily dependent on the existence of prescriptive jurisdiction.A State's enforcement jurisdiction within its own territory is presumptively absolute over all matters and persons situated therein. The State's legislative enactments primarily reflect its prescriptive jurisdiction.

2. What are the principles associated with extra-territorial jurisdiction vis-à-vis cyber laws?

The principles associated with extra-territorial jurisdiction vis-à-vis cyber laws are as follows:-

- Territorial principle

- Nationality Principle

- Protective Principle

- Passive Personality Principle

- Universality principle

3. What is meant by the 'Effects Doctrine'?

The Effects Doctrine is an extra-territorial application of national laws where an action by a person with no territorial or national connection with a State has an effect on that State.

4. What are the tests involved in determining jurisdiction?

The tests involved in determining jurisdiction in instances involving disputes of cyber laws are as follows:

- Minimum Contacts Test

- Purposeful availment Test

- Sliding Scale Test

5. What is understood by 'personal jurisdiction' in context of cyberspace?

Personal Jurisdiction is the competence of a court to determine a case against a particular category of persons (natural as well as juridical) involving a dispute arisen associating with cyberspace. This can comprise of either general jurisdiction or specific jurisdiction.

1.12 ACTIVITY

*"The effectiveness of any judicial system rest on the bedrock of jurisdiction itself".*Explain the jurisdiction issues in Internet-based on US law as well as Indian law. (2000-2500 words)

Unit 2: Best Practices of Cyber Law across the World

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- How cyber law is being implemented in the countries - USA, UK, Canada and Australia
- The policies and laws which are effective in creating and maintaining a safe cyber space.
- The policies and laws which are the best practices and can be inculcated in our country for reference.

1.2 INTRODUCTION

There are more than 7 billion people in this world with almost 50% on as an internet user. This number keeps on increasing exponentially, every single day. This generation can be called the internet generation and the century being the internet century. For a while we can imagine our lives without food or water but surviving without internet for hours seems impossible. Today we connect with our family, friends, peers and everyone else in the world through the internet

creating and implementing in true sense the idea of a global village without borders. World connectivity has brought about such a revolution that the post-net and pre-net worlds are entirely unrecognizable. With the increasing popularity of online activities, the rate of online crimes has also increased exponentially. While the extent and impact of these crimes vary greatly across the globe but in totality it has become a universal nuisance. From cyber bullying to cyber terrorism, newer technology is providing fertile lands for newer crimes.[23]

Understanding and having knowledge about the cyber law of various countries is extremely crucial because cyber space is not restricted to the territorial understanding of a state, rather is spread across the globe without much demarcations. It touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. cyber activities are not governed by geographical borders, which makes dealing with such crimes all the more confusing and complex and therefore, a lot of cyber-crimes go unreported. Apart from the International law and guidelines in this field, it is also important to understand how the other jurisdictions work in order to check this invisible vast omnipresent space.[24]

1.3 USA

The United States have been a prime sufferer of cyber-crime in the world. However, it has devised a very strong cyber law in place and keeps working and updating that with the very speed of technology transformation. Around sixty percent of cyber cries are filed in the USA have been convicted and sentenced. The cyber laws and privacy system of the States is arguably the oldest, most robust and effective in the world.

The Computer Fraud and Abuse Act of 1986 (CFAA), enacted into law today as United States Code Title 18 Section 1030 (18 U.S.C. §), is the primary federal law governing cybercrime in the United States. n the 1970s and early '80s, many phone phreaks and early computer hackers ran rampant through online systems unhampered by worries of legal complications. CFAA was

[23]Cyber Laws: What Have Different Countries Done <https://unbumf.com/cyber-laws-what-have-different-countries-done-to-prevent-cyber-crime/>

[24]Miguel Mendoza and Miguel Mendoza, 'Challenges And Implications Of Cybersecurity Legislation | Welivesecurity' (*WeLiveSecurity*, 2020) <https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/>

aimed at criminal offences and did not cover civil offences by then. It offered a powerful set of prosecutorial tools to address criminal uses of computer.[25]

It criminalised spreading of malevolent code, trading in passwords or other access control mechanisms etc. The act defines a category of "protected computer" to exclude and safeguard the federal interest but in theory and through princely elucidation all the computers are covered.

The Act has been amended over the years to refine the definitions and to expand coverage into other aspects of cybercrime. Between 1988 and 2008, the law was amended 9 folds. A lot of updates included mounting security to financial institutions and other private computers, including civil actions, adding tampering and attempted extortion, criminalising of taking information off of systems etc.[26]

The important provisions under this law are:

S. No.	Section Number	Act - The Computer Fraud and Abuse Act of 1986 (CFAA)
1	**1028**	**Fraud and related activity in connection with identification documents, authentication features, and information**
2	**1028A**	**Aggravated identity theft**
3	**1029**	**Fraud and related activity in connection with access devices**
4	**1030**	**Fraud and related activity in connection with computers**
5	**1037**	**Fraud and related activity in connection with electronic mail**
6	**1343**	**Fraud by wire, radio, or television**
7	**1362**	**Malicious mischief related to communications lines, stations, or systems**

[25]Kamble, R (2013). CYBER LAW AND INFORMATION TECHNOLOGY.International Journal of Scientific and Engineering Research. 4. 789-794

[26]Eichensehr, Kristen, The Cyber-Law of Nations (January 8, 2014) 103 Geo L J 317 (2015)

8	**1462**	**Importation or transportation of obscene matters**
9	**1465**	**Transportation of obscene matters for sale or distribution**
10	**1466A**	**Obscene visual representation of the sexual abuse of children**
11	**2251**	**Sexual exploitation of children**
12	**2252**	**Certain activities relating to material involving the sexual exploitation of minors**
13	**2252A**	**Certain activities relating to material constituting or containing child pornography**
14	**2252B**	**Misleading domain names on the Internet [to deceive minors**
15	**2252C**	**18 U.S.C. §– Misleading words or digital images on the Internet**
16	**2425**	**Use of interstate facilities to transmit information about a minor**
17	**2319**	**Criminal infringement of a copyright**
18	**2510-2522**	**Interception of wire, oral, or electronic communication**
19	**2701-2712**	**Preservation and disclosure of stored wire and electronic communication**
20	**3121-3127**	**Pen registers and trap and trace devices**

The Electronic Communications Privacy Act, 1986 allows the government to access digital communications such as email, social media messages, information on public cloud databases, and more with a summon. No warrant is required if the items in question are 180 days old or older.

Cyber Intelligence Sharing and Protection Act (CISPA), 2011 was reintroduced in 2015 at the Parliament as an amendment to the National Security Act of 1947. This was set up with the objective of improving cybersecurity by sharing information on potential cyber threats with the federal government.

Children's Online Privacy Protection Act (COPPA), 2012 was implemented in 2013 which mandated websites that gather data on children under the age of thirteen to conform with the Federal Trade Commission (FTC), which governs whether a website is suitable for children by reviewing its language, content, advertising, graphics and features, and intended audience.

It can be concluded that US has some pretty high levels of security when it comes to cyber safety and the cyber laws are much varied and comprehensive. the government has been working to introduce stricter laws to equip organizations to secure the data from the latest cyber threats. In conclusion one can say that USA does set a good example for cyber laws and security across the world.[27]

In the year 2014, these new legislations were introduced:

S. No.	Legislation
1	**National Cybersecurity Protection Act (NCPA)**
1	**Cybersecurity Enhancement Act of 2014 (CEA)**
2	**Federal Information System Modernization Act of 2014 (FISMA 2014)**
3	**Cybersecurity Workforce Assessment Act (CWWA)**
4	**Border Patrol Agent Pay Reform Act (BPAPRA)**

1.4 UK

The United Kingdom has been fighting issues of cyber-crime and cyber security over a lot of years. Most recently the case of ***'Cambridge Analytica'*** also dwelled around the Data Protection laws and brought about a new regulation for the European Union. In UK, there is a demarcation between two types of cyber- crimes. They differentiate between a cyber-enabled crime and a cyber-centric crime. Cyber-centric crimes are things like unauthorised access to computer systems, new crimes brought about through the existence of computers. However, cyber-enabled

[27] WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009), available at <http://www.whitehouse.gov/assets/ documents/Cyberspace_Policy_Review_final.pdf>

crimes are crimes that have always existed, but benefit from the existence of computers such as fraud.[28]

The list of significant legislations specifically for cyber-crimes is:[29]

S. No.	Legislation	Purpose
1.	**Malicious Communications Act 1988**	**It dealt with communication and its malice and offense caused**
2.	**Official Secrets Act 1989**	**It deals with national security**
3.	**Computer Misuse Act 1990**	**It specifies various hacking offences**
4.	**Data Protection Act 1998**	**It implements the Data Protection Directive 1995**
5.	**Communications Act 2003**	**It is the main source of UK telecommunications law**
6.	**Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)**	**It regulated the communication and data protection for electronic communication.**
7.	**Serious Crime Act 2015**	**It defines principles for the protection of data**

The Computer Misuse Act, 1990 (CMA) is the chief piece of UK legislation relating to offences or attacks against computer systems such as hacking or denial of service. The act left space for technological advancement and did not define a 'computer'. In ***DPP v McKeown and, DPP v Jones [1997] 2 Cr App R 155 HL,*** Lord Hoffman defined computer as 'a device for storing, processing and retrieving information'; this means that a mobile smartphone or personal tablet device could also be defined as a computer in the same way as a traditional 'desk-top' computer or 'PC'. There is jurisdiction to prosecute all CMA offences if there is "at least one significant link with the domestic jurisdiction" (England and Wales) in the circumstances of the case."

[28] GOV'T OF KENYA, CYBERSECURITY STRATEGY 12 (2014), available at <http://www.icta.go.ke/wpcontent/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf>

[29] U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 11 (2011), available at <https://www.gov.uk/government/publications/cyber-securitystrategy>

Offences under the Computer Misuse Act are tabled below:

S. No.	Section Number	Act - The Computer Misuse Act, 1990 (CMA)
1	**1**	**Unauthorised access to computer material, it involves 'access without right' along with an intention for such**
5	**2**	**Unauthorised access with intent to commit or facilitate commission of further offences**
6	**3**	**Unauthorised acts with intent to impair the operation of a computer**
7	**3ZA**	**Unauthorised acts which tend to attack the critical national infrastructure**
8	**3A**	**It deals with those who make or supply malware.**

This act has been amended twice, by the Police and Justice Act 2006 and by the Serious Crime Act 2015.

Data Protection Act 1998 creates criminal offences that may be committed alongside cyber-dependent crimes inclusive of procuring or revealing personal data, disclosure of personal data, entailing private data for selling or offering to sell it etc.

Communications Act, 2003magnifies our understanding of our ambit of malicious and offensive communication. It also includes that when one sends through a 'public electronic communications network' a message or other matter that is 'grossly offensive' or of an 'indecent, obscene or menacing character', it is an offence. To send or false message 'for the purpose of causing annoyance, inconvenience or needless anxiety to another' is also an offence. It involves the acts of cyber bullying, cyber trolling, virtual mobbing etc.[30]

Serious Crime Act 2015 covers processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For monitoring and recording of communications in transit an artificial person must consider the act.

[30] C Matthew, Waxman Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE J INT'L L, volume 421, p 431 – 468 Posted: 2011

Certain other laws relating to this field in this particular jurisdiction are Police and Justice Act 2006, EU Directive 2013/40/EU, Terrorism Act 2000, Regulation of Investigatory Powers Act 2000, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Human Rights Act 1998, Extradition Act 2003, Crime and Courts Act 2013, Telecommunications (Data Protection and Privacy) Regulations 1999 etc.

UK is working towards betterment of cyber security and data protection each day. Presently on May 2018 the General Data Protection Regulation 2016/679 (GDPR) became directly effective in the UK and the Network and Information Security Directive 2016/1148 to be implemented in all member states of the European Union. But Brexit puts everything under much speculation and uncertainty.

1.5 CANADA

Canadian cyber laws are generally principles-based which provides organisations more tractability whilst covering the possible crimes. Canadian approach to Cyber Security is much more comprehensive with a lot of regulations being the responsibility of government agencies as well as private sectors.[31]

There are many legislations and regulations for such including Cybersecurity Best Practices Guide and a Cyber Incident Management Planning Guide 2015 launched by the Investment Industry Regulatory Organization, the Bulletin on Cybersecurity 2016 by Mutual Fund Dealers Association of Canada, Security Self-Assessment Tool by the Office of the Privacy Commissioner of Canada etc.[32]

Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) applies to the private sector to protect personal information within their possession or control. It contains implicit or explicit accountability and security obligations for personal information by federally-regulated organizations. PIPEDA was amended in 2015 was amended to ensure that any breach be reported to Office of the Privacy Commissioner of Canada. Also, the breaches have to be

[31] Eloise F Malone & Michael J Malone, "The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response" (2013) 19:2 Can Foreign Policy J 158 at 171

[32] Greg Weston "Foreign hackers attack Canadian Government", CBC News (16 February 2011), online: [perma.cc/Y4D3-QHLB]

reported and maintained. Knowledge of such crime and failing to report is also an offence under the act.

Bill C-59 Act, 2017 was introduced to enlarge the authorization of the Communications Securities Establishment (CSE). The act allowed the CSE authorities to interfere with foreign online efforts that threaten the country by shielding Canada's networks from foreign cyber threats – both defensively and actively. It would include degrading, disrupting, influencing, responding to or interfering with the capabilities, intentions or activities of a foreign actor.[33]

Canada has created the ***National Cyber Security Strategy*** ***and a National Cybercrime Coordination Unit,*** which coordinates for cyber-crime investigations in the country and partners internationally. They also provide digital investigative advice to Canadian law enforcement; and establish a national reporting mechanism for Canadian citizens and businesses to report cybercrime incidents. Moreover, the Canadian Anti-Fraud Centre mitigates public marketing fraud.

In the year 2012, the Ontario Court of Appeal acknowledged "intrusion upon seclusion", as tort in which "one who intentionally or recklessly intrudes, physically or otherwise, upon the seclusion of another or his or her private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person".

In the year 2016, the Ontario Court of Appeal acknowledged another privacy-related tort in ***Jane Doe 464533 v ND,*** in which, "one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."

Therefore, in Canada apart from considering cyber-crimes as criminal offence, through introducing such torts, the court adopted it as a civil offence too. It helped to establish that with the speeding technology, the need for recognition and laws to move equally fast is significant. Lawsuits involving data breaches also include more traditional allegations, such as claims of negligence, breach of contract and statutory breach.

[33] Public Safety Canada, National Cyber Security Strategy, (Ottawa: Public Safety Canada, 2018), online (pdf): [perma.cc/23W4-5MER] at 2

1.6 SUGGESTIONS DERIVED FROM BEST PRACTICES ACROSS THE WORLD

There is so much to learn from the various countries and practices about safeguarding our nation from cyber-crime and cyber terrorism. To help one understand, here are a few suggestions which can be implemented in India for a betterment in the cyber security world.

1. A tiered cybersecurity policy can be drafted. The written policy will act as a formal guide to all cybersecurity measures used in an organisation. It helps keep everyone on the loop and create a workflow which can be monitored and maintained ensuring that the levels of cyber security are maintained at every level and thereby in the entire organisation and consequently country.
2. Regulating and keeping a backup of data and maintaining a record of all the data is equally important to ensure that the data remains safe, unaltered and non-destroyable. Through regulations it must be ensured that this backed up data is thoroughly protected, encrypted and frequently updated. It is also imperative to divide backup duty among several people to mitigate insider threats.[34]
3. Partnership with other countries helps a lot in dealing with cyber-crimes as the boundary does not restrict such kind of security issues. If a country can partner with other countries and develop a system within themselves to ensure cyber security and protection against cyber-attacks, it will be way more fruitful than processing it individually.
4. Mass awareness to ensure that cyber-security is understood, dealt and tackled individually by each person is extremely crucial to ensure safety from cyber-crimes. Regulation for such can be drafted and trainings at large for public be done to ensure, everyone understand and follows those regulations can help a country at large.[35]

1.7 LET'S SUM UP

In this chapter, we have studied how cyber law is being implemented in countries like USA, UK and Canada. We also studied about the policies and laws which are effective in creating and

[34]Cyberbullying and the Law | MediaSmarts
<https://mediasmarts.ca/digital-media-literacy/digital-issues/cyberbulling/cyberbullying-law>
[35]Remarks by Director David Vigneault at the Economic Club
https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html

maintaining a safe cyberspace. Finally, we ended out discussion with the best practices that can be inculcated in our country.

1.8 FURTHER READING

- Singh, Umrav. (2016). Cyber Laws in India.
- Cyber Laws of Different Countries - Cyberlaws.Net, Cyberlaws.Net (2019), http://cyberlaws.net/cyber-law-repository/cyber-laws-different-countries/ (last visited Nov 24, 2019).
- Cis-india.org (2019), https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf (last visited Nov 24, 2019).
- (2019), https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=10766&context=theses (last visited Nov 24, 2019).

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is objective of the Computer Fraud and abuse Act, 1986?**

CFAA was aimed at criminal offences and did not cover civil offences by then. It offered a powerful set of prosecutorial tools to address criminal uses of computer.

2. **What does Canadian cyber laws mainly focus on?**

Canadian cyber laws are generally principles-based which provides organizations more tractability whilst covering the possible crimes. Canadian approach to Cyber Security is much more comprehensive with a lot of regulations being the responsibility of government agencies as well as private sectors.

3. **Why was Serious Crimes Act, 2015 introduced?**

Serious Crime Act 2015 covers processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For monitoring and recording of communications in transit an artificial person must consider the act.

1.10 ACTIVITY

Elucidate the different laws and policies introduced by other countries and how it can be implemented in India along with a reason? (1000 – 1500 words)

Unit 3: The Appellate Tribunal and Latest Amendments

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Establishment of Appellate Tribunal
- Latest Amendments
- Overview of Telecom Regulatory Authority of India

1.2 INTRODUCTION

Cyber Appellate Tribunal was established under the Information Technology Act, 2000 under the aegis of Controller of Certifying Authorities (CCA). It was a ***'multi-member body'.*** The Tribunal has the statutory authority to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Act. The new amendments have made the Tribunal an ***'expert body'***consisting of members having varied qualifications to appreciate the legal, technical and factual questions involved in the appeals in the first appellate stage itself.[36]

1.3 ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL

The InformationTechnology Act of India, which regulates several important aspects of electronic information, including the regulation of privateelectronic transactions as well as detailing civil and criminaloffences relating to computers and electronic information, contemplates a specialized dispute resolution mechanism for disputesrelating to the offences detailed under the Act. The Act provides forthe establishment of quasi-judicial bodies, namely adjudicatingofficers under ***Section 46,*** to hear disputes namely, offences of a civil nature under ***Section 43, 43A, 44 and 45 of the Act,*** as well ascriminal offences. The adjudicating officer has the power to bothaward compensation as damages in a civil remedy, as well as imposepenalties for the contravention of the Act, and therefore has powers of both civil and criminal courts. The first appellate body provided inthe Act, i.e. the authority that any party not satisfied by the decisionof the adjudicating officer can appeal to, is the Cyber AppellateTribunal, consisting of a Chairperson and any other members soprescribed by the Central Government. The second appeal, if a partyis aggrieved by the decision of the Cyber Appellate Tribunal, may befiled before the High Court having jurisdiction, within 60 days fromthe date of communication of the order. The proper functioning of theCyber Appellate Tribunal is particularly necessary for thefunctioning of a just judicial system in light of the provisions of theInformation Technology Act.

[36]Cyber Appellate Tribunal and its powers – Unit 6 – MyBSCIT.com <https://www.mybscit.com/cyber-law/cyber-appellate-tribunal-and-its-powers-unit-6>

As per ***Section 48 of the Act,*** the Central Government provides for an appointment of one or more appellate tribunals but the language of the ***Rule 13 of the Cyber Regulations Tribunal (Procedure) Rules, 2000*** makes it clear that there shall only be one tribunal and it shall ordinarily hold its sittings at New Delhi.[37] The said rule has further provided a lot of flexibility to Cyber Appellate Tribunal as far as its sittings are concerned. It is for the Chairperson to exercise this ***'rule of sittings'*** in a most appropriate and judicious manner. The Tribunal shall notify to the parties the date and the place of hearing of the application ***(Rule 12).*** Initially, the Tribunal consisted of only one person who was referred to as the Presiding Officer and was to be appointed by way of notification by the Central Government.[38]

It is for the Central Government to specify by order the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction. It was held by the Supreme Court in ***Union of India v Paras Laminates (P) Ltd.,***[39] "There is no doubt that the Tribunal functions as a court within the limits of its jurisdiction. It has all the powers conferred expressly by the statute. Furthermore, being a judicial body, it has all those incidental and ancillary powers which are necessary to make fully effective the express grant of statutory powers". The powers of the Tribunal are no doubt limited. Its area of jurisdiction is clearly defined, but within the bounds of its jurisdiction, it has all the powers expressly and impliedly granted.

1.4 LATEST AMENDMENTS

For the smooth functioning of any law, such law must be just,fair and reasonable and at the same time there must be aproper forum to regulate it. To give effect to the Information Technology Law, theparliament has established the most important authoritiesunder the same Act for smooth functioning. It has been rightly said by Aristotle that ***"It is better for a city to be governed by a good man than even by good laws".***

[37]THE CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE) RULES <https://law.cyberpandit.org/rule02/>
[38]A Review of the Functioning of the Cyber Appellate Tribunal <https://cis-india.org/internet-governance/blog/review-of-functioning-of-cyber-appellate-tribunal-and-adjudicatory-officers-under-it-act>
[39]*Union of India v Paras Laminates (P) Ltd*, [1990] 4 SCC 453

The Finance Act, 2017 has made several structural changes including the merging of eight powerful and autonomous administrative tribunals with other tribunals. The Government of India has moved an amendment which it proposed that the Cyber Appellate Tribunal constituted under Section 48 of the IT Act would be merged with ***Telecom Disputes Settlement & Appellate Tribunal (TDSAT)*** constituted under Section 14 of the Telecom Regulatory Authority of India (TRAI) Act.[40]

The Cyber Appellate Tribunal has not been functioning since June 2011. The jurisdiction of TDSAT extends to matters that lay before the Cyber Appellate Tribunal and also the Airport Economic Regulatory Authority Appellate Tribunal. The Tribunal exercises original as well as appellate jurisdiction in regard to Telecom, Broadcasting and Airport tariff matters. With respect to cyber matters the Tribunal exercises only the appellate jurisdiction.

The TDSAT consists of a Chairperson and two members appointed by the Central Government. Section 14C of the Act discusses about the Qualifications for appointment of Chairperson and Members.

1.5 OVERVIEW OF TELECOM DISPUTES SETTLEMENT AND APPELLATE TRIBUNAL

Telecom Regulatory Authority of India (TRAI) was enacted in 1997. TRAI is empowered to adjudicate upon disputes among service providers or between the service providers and a group of Consumers on matters relating to technical compatibility and interconnection between the Service Providers, revenue sharing arrangement between Service Providers and quality of telecommunication services and interests of consumers. TRAI was vested with the power to issue directions to the Service Providers. Appeals from the decisions of TRAI lay to the High Court and appeals therefrom lay to the Supreme Court. The jurisdiction of civil courts was barred.

In respect of Telecom, Broadcasting and Airport tariff matters, the Tribunal's orders can be appealed to the Supreme Court but only on substantial questions of law. However, no appeal lies against an interlocutory order or against any decision or order made by the Tribunal with the

[40]Probity in Governance in India
<http://www.legalserviceindia.com/articles/nkdev.htm>

consent of the parties. In regard to Cyber matters, the Tribunal's order can be appealed before High Court.[41]

1.6 INTRODUCTION TO TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL (TDSAT)

The Telecom Regulatory Authority of India Act, 1997 was amended by the Telecom Regulatory Authority of India (Amendment) Act, 2000. The amendments were introduced to resolve the issues that -emerged from the implementation of the Act. The desired objectives of bringing about functional clarity, strengthening the regulatory framework and the disputes settlement mechanism were attained by bringing about a clear distinction between the recommendatory and regulatory functions of the Telecom Regulatory Authority of India (TRAI) by making it mandatory for the Government to seek recommendations of TRAI in respect of specified matters and by the setting up a separate dispute settlement mechanism etc. An Appellate Tribunal known as the "Telecom Disputes Settlement & Appellate Tribunal" has been set up under Section 14 of the Telecom Regulatory Authority of India Act, 1997 as amended by TRAI (Amendment) Act, 2000 to adjudicate disputes and dispose of appeals with a view to protect the interests of service providers and consumers of the telecom sector and to promote and ensure orderly growth of the telecom sector. The Appellate Tribunal came into existence on 29 May 2000 and started hearing cases from January 2001.

The functions of the appellate tribunal are to adjudicate any dispute between a licensor and a licensee, between two or more service providers, between a service provider and a group of consumers, and to hear and dispose of appeals against any decision or order of TRAI, DoT and MIB. The appellate tribunal consists of a Chairperson and two Members.

1.7 FORMATION OF TDSAT

In order to bring in functional clarity and strengthen the regulatory framework and the disputes settlement mechanism in the telecommunication sector, the TRAI Act of 1997 was amended in the year 2000 and TDSAT was set up to adjudicate disputes and dispose of appeals with a view

[41]Current based PRELIMS QUESTION 19 MARCH 2020 | The Core IAS <https://thecoreias.com/current-based-prelims-question-19-march-2020/>

to protect the interests of service providers and consumers of the telecom sector and to promote and ensure orderly growth of the telecom sector. In January 2004, the Government included broadcasting and cable services also within the purview of TRAI Act. After coming into force of the relevant provisions of the Finance Act 2017, the jurisdiction of TDSAT stands extended to matters that lay before the Cyber Appellate Tribunal and also the Airport Economic Regulatory Authority Appellate Tribunal.

1.8 COMPOSITION OF TDSAT

The Tribunal consists of a Chairperson and two Members appointed by the Central Government. The Chairperson should be or should have been a Judge of the Supreme Court or the Chief Justice of a High Court. A Member should have held the post of Secretary to the Government of India or any equivalent post in the Central Government or the State Government for a period of not less than two years or a person who is well versed in the field of technology, telecommunication, industry, commerce or administration.[42]

1.9 POWERS AND JURISDICTION

The Tribunal exercises jurisdiction over Telecom, Broadcasting, IT and Airport tariff matters under the TRAI Act, 1997 (as amended), the Information Technology Act, 2008 and the Airport Economic Regulatory Authority of India Act, 2008. The Tribunal exercises original as well as appellate jurisdiction in regard to Telecom, Broadcasting and Airport tariff matters. In regard to Cyber matters the Tribunal exercises only the appellate jurisdiction.

1.10 PROCEDURE

- The Tribunal is not bound by the procedure laid down by the Code of Civil Procedure, 1908;
- It has the power to regulate its own procedure;
- It is to be guided by the principles of natural justice;

[42]Telecom Disputes Settlement & Appellate Tribunal (TDSAT)
<https://www.insightsonindia.com/2018/12/14/telecom-disputes-settlement-appellate-tribunal-tdsat/>

Tribunal has the same powers as are vested in a civil court under the CPC in respect of:

a) summoning and enforcing the attendance of any person and examining him on oath;
b) requiring the discovery and production of documents;
c) receiving evidence on affidavits;
d) subject to the provisions of sections 123 and 124 of the Indian Evidence Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office;
e) issuing commissions for the examination of witnesses or documents;
f) reviewing its decisions;
g) dismissing an application for default or deciding it ex parte;
h) setting aside any order of dismissal or any application for default or any order passed by it ex parte; and
i) any other matter which may be prescribed.

In addition, the Tribunal can call for the records relevant to disposing of a Petition or appeal, for the purpose of examining the legality or propriety or correctness of any decision or of any order etc. of TRAI.

1.11 NATURE OF PROCEEDINGS

- The Tribunal is the Court of first instance except cyber matters.
- Every proceeding before the Tribunal is deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196, of the Indian Penal Code (45 of 1860);
- The Tribunal is deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).
- Tribunal's Orders are executable as a decree of civil court.

1.12 Appeals

In respect of Telecom, Broadcasting and Airport tariff matters, the Tribunal's orders can be appealed to the Supreme Court but only on substantial questions of law. However, no appeal lies

against an interlocutory order or against any decision or order made by the Tribunal with the consent of the parties. In regard to Cyber matters, the Tribunal's order can be appealed before High Court.

1.13 LET'S SUM UP

In this chapter, we have studied the concept of Cyber Appellate Tribunal along with its establishment and procedure and powers. Furthermore, we also studied when a matter can be appealed to Cyber Appellate Tribunal. Finally, we ended our discussion the latest amendments that took place in appellate tribunal and also the overview of Telecom Disputes Settlements and Appellate Tribunal.

1.14 FURTHER READING

- Krishisanskriti.org (2019), https://www.krishisanskriti.org/vol_image/22Oct2015061009zzzzzzzzzzzzzzzzzLOVE%20KUMAR%20GUPTA%20%20%20%20%20%20%20%20%20120-122.pdf (last visited Nov 22, 2019).
- A Review of the Functioning of the Cyber Appellate Tribunal and Adjudicatory Officers under the IT Act — The Centre for Internet and Society, Cis-india.org (2019), https://cis-india.org/internet-governance/blog/review-of-functioning-of-cyber-appellate-tribunal-and-adjudicatory-officers-under-it-act (last visited Nov 22, 2019).
- http://www.tdsat.gov.in/admin/introduction/uploads/TDSAT%20INTRO.pdf

1.15 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the cyber appellate tribunal?**

Cyber Appellate Tribunal was established under the Information Technology Act, 2000 under the aegis of Controller of Certifying Authorities (CCA). It is a *'multi-member body' having* the statutory authority to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Act.

2. When was TRAI enacted?

Telecom Regulatory Authority of India (TRAI) was enacted in 1997.

3. What is the Composition of TDSAT?

The Tribunal consists of a Chairperson and two Members appointed by the Central Government.

4. What was the latest amendments that took place in the Cyber Appellate Tribunal?

The Finance Act, 2017 has made several structural changes including the merging of eight powerful and autonomous administrative tribunals with other tribunals. The Government of India has moved an amendment which it proposed that the Cyber Appellate Tribunal constituted under Section 48 of the IT Act would be merged with ***Telecom Disputes Settlement & Appellate Tribunal (TDSAT)*** constituted under Section 14 of the Telecom Regulatory Authority of India (TRAI) Act.

The Cyber Appellate Tribunal has not been functioning since June 2011. The jurisdiction of TDSAT extends to matters that lay before the Cyber Appellate Tribunal and also the Airport Economic Regulatory Authority Appellate Tribunal. The Tribunal exercises original as well as appellate jurisdiction in regard to Telecom, Broadcasting and Airport tariff matters. With respect to cyber matters the Tribunal exercises only the appellate jurisdiction.

1.12 ACTIVITY

Explain the constitution of Cyber Appellate Tribunal along with the latest amendments? What are the powers and functions of TDSAT? (1000 words)

Unit 4: Facets of Cyber Crime: Offences, Penalties and Compensation

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Doctrine of Actus Reus and Mens Rea in Cybercrimes

- Facets of Cyber Crime
- Legislative Framework and Position in India

1.2 INTRODUCTION

The rampant growth and development of Internet and Computer technology have paved the way to new forms of transnational crimes, especially Internet-based. The Indian Legislature does not provide the explicit definition of Cybercrime in any statute. In general, the term cybercrime means any kind of illicit activity which is carried out with the help of the internet or computers. It includes all unauthorized access of information and security breakage like privacy, password etc. with the aid of the Internet. On the whole, Cybercrime is an unlawful act wherein the computer is either used as a tool or a target or both.[43]

1.3 DOCTRINE OF ACTUS REUS AND MENS REA IN CYBERCRIMES

There are two essential elements which constitute a crime i.e., Actus Reus and Mens Rea.

- ***Actus Reus in Cyber Crimes***

  The word 'Actus' connotes a 'mental or spiritual act'. Actus Reus can be defined as "Such result of human conduct as the law seeks to prevent". Actus Reus in case of cybercrimes has become a challenging task as the entire act is committed in intangible surroundings. The element of actusreus is relatively easy to identify, but it is very difficult to prove. One must-see at what state of mind the wrongdoer has committed the crime and must be able to prove that the doer was well aware of the unauthorized access.

- ***Mens Rea in Cyber Crimes***

  Mens Rea is the second essential element in a crime and is known as 'guilty mind'. It refers to the mal-intent of the individual who commits the act. Mensrea in case of Cybercrimes

[43] Jain, Neelesh&Shrivastava, Vibhash& Professor, & Professor, Assistant (2014) "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY" 4

encompasses two elements. Firstly, there must be an 'intent' to secure access to any kind of programme or data held in any computer, computer system or network. Secondly, the person committing such offence must have the knowledge that the access he intends to secure is unauthorized.[44]

1.4 FACES OF CYBERCRIME

- ***Hacking:*** Hacking means unauthorized access/control over a computer system or a computer network. An act of hacking completely destroys the data as well as computer programmes.
- ***E-mail Spoofing:*** A spoofed e-mail is one which misrepresents its origin i.e., it is an e-mail that appears to originate from one source while it actually has been sent from another source. In 2016, Flipkart's CEO BinnyBansal's email account was spoofed.
- ***Trojan Attacks:*** A Trojan is an unauthorized programme which passively gains control over another's system by representing itself as an authorized programme. The most common form of installing a Trojan is via e-mail.
- ***Salami attacks:*** This type of crime is normally prevalent in financial institutions in instances of financial crimes. It is also known as Salami Slicing wherein the attackers use an online database to seize the personal information of the customers such as bank details, credit card details etc. Later, the attackers keep deducting small amounts of money from every account over a stipulated period of time.[45]
- ***Data Diddling:*** Data diddling involves changing of data prior to or during input into a computer i.e., alteration of raw data before a computer processes it and then changing it back after the processing is completed. Section 66 and 43(d) of the I. T. Act, 2000 covers the offence of data diddling. The NDMC Electricity Billing Fraud Case[46] that took place in 1996 is a typical example. A private contractor was made to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized

[44]Etter, B (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide
[45]Etter B (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand
[46]2003 IIAD Delhi 452

accounting, record maintenance and remittance in his bank was misappropriated by manipulating data files to show less receipt and bank remittance.

- ***Intellectual Property Crimes:*** Crimes pertaining to IPR includes software piracy, copyright infringement, trademark violations, theft of computer source code etc. One such crime is Domain Name violations and passing off. In Cardservice International Inc. VsMc Gee[47], it was held that the domain serves the same function as the trademark and is not a mere address or like finding the number on the Internet and, therefore, it is entitled to equal protection as a trademark. It was further held that a domain name is more than a mere Internet address for it also helps identify the Internet site for those who reach it, much like a person's name identifies a particular person.
- ***Phishing and Vishing:*** Phishing means the acquisition of information such as usernames, passwords, credit card details etc. by electronic communication. The information is acquired by using fake emails or fake messages which contain link of virus / malware infected fake websites. This kind of websites request the users to enter all their personal details. On the other hand, Vishing is typically used to steal credit card numbers or other kind of information from the users for use in instances of identity theft.[48]

1.5 CYBER PORNOGRAPHY

The word 'Pornography' has no specific definition in the eyes of law as every country has its own customs and traditions. Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials The act pornography is made legal in some countries but in others, it is illegal and banned. The Indian legal system has been structured in such a way that it contains provisions to criminalize any kind of scatological content.[49] Legalization of Child Pornography doesn't come under the purview of

[47] *Cardservice International Inc vMc Gee*, 42 USPQ 2d 1850

[48] Eric JSinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2

[49] See e g The Post Office Act, 1893 (prohibits obscene matters being transmitted through post); The Sea Customs Act, 1878 (prohibits the import of obscene literature); The Dramatic Performances Act, 1876 (prohibits obscene plays); The Cinematograph Act, 1952 (makes provisions for censorship of films); The Press Act, 1951 (prohibits grossly indecent, scurrilous or obscene publications); The Indecent Representation of Women (Prohibition) Act, 1986 (prohibits obscene photographs of women)

pornography as a whole. Child Pornography at the very instance is a felonious act and is one of the heinous crimes that has eventually led to other severe crimes such as sex tourism, sexual abuse of child etc. The obscene contents involving children creates a major threat to the development and security of children which initiates a path for sexual abuse of children. The concepts of obscenity and pornography oscillate from time to time and from country to country. Although the terms obscenity and pornography are different, they are related to each other.

1.6 TEST DETERMING OBSCENE CONTENT

The test of obscenity was first laid down in ***Regina VsHicklin***[50] ***(also known as Hicklin's test***i.e., a content is obscene if "the tendency of the matter charged with obscenity is to deprave and corrupt those whose minds are open to such immoral influences and whose hands a publication may fall". This approach was later adopted even in India in the case of ***Ranjit Singh UdeshiVs State of Maharashtra***[51] with regards to a sale of an allegedly obscene magazine.

After the Hicklin's Test, the U.S Supreme Court went against the said rule and established a new set of principles called as the ***Community Standards Test*** **in** ***Roth Vs. United States***[52] and held that "obscene material was not protected by the First Amendment and could be regulated by the States rather than by a singular, Federal standard and also a new judicial standard for defining obscenity that invoked the average person's application of contemporary community standards to judge whether or not the dominant theme of the material taken as a whole appeals to prurient interest". Furthermore, the Supreme Court held that in order to decide how obscenity derived, we need to consider the following five-part structure:-

- The perspective of evaluation is that of an ordinary, reasonable person.
- Community Standards of acceptability are used to measure obscenity.
- Obscenity law only applies to the works whose themes are in question.
- A work, in order to be evaluated for obscenity, has to be taken in its entirety.

[50] *Regina vHicklin* [1868] LR 3 QB 360
[51] *Ranjit Singh Udeshi v State of Maharashtra* AIR [1965] SC881
[52] *Community Standards Test* in *Roth v United States*[1957]354 U S476

- An obscene work is one that aims to excite individuals' prurient interest.

However, in ***Samresh Bose VsAmalMitra***[53]**,**the Supreme Court held that 'vulgar writing is not necessarily obscene'. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novels; whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences. In the instant case, the court had differentiated between vulgarity and obscenity and further held that while judging the question of obscenity 'the Judge should place himself in the position of a reader of every age group in whose hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers'.

This Community Standards Test was also used in India in, ***K.A. Abbas Vs Union of India***[54]which stated that;

- The dominant theme taken as a whole, appeals to prurient interests according to the contemporary standards of the average man;
- The motion picture is not saved by any redeeming social value; and
- It is patently offensive because it is opposed to contemporary standards.

Later, the Millers Test was brought to light which was a developed form of Community Standards Test. The Millers Test took birth from the case of ***Miller Vs California***[55]whereinThe Supreme Court of United States provided the basic guidelines and three-point tests to determine obscenity in the work. They are as follows:-

- That the average person, applying contemporary 'community standards', would find that the work, taken as a whole, appeals to the prurient interest.
- That the work depicts or describes, in an offensive way, sexual conduct or excretory functions, as specifically defined by applicable state law or applicable law.
- That the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

[53]*Samresh Bose vAmalMitra* AIR [1986] SC 967
[54]*K.A. Abbas v Union of India* AIR [1971] SC481
[55]*Miller v California* 413 US 15 [1973]

1.7 PRESENT SCENARIO IN INDIA

The Supreme Court of India presently adopts the *Community Standards Test* as a measure of detecting obscene content. In ***AveekSarkar V. State of West Bengal***[56]**,** the facts of the case revealed that a German magazine published an article about a tennis player picturing him naked with his fiancé as a stand against racism and to show that love champions over everything. The Supreme Court found the respondents innocent of the charges levied against them and held that in a situation like this Hicklin's test cannot be used and the only measure to be implemented is the community standards test; and it further stated that the photograph must be viewed in the context of the message which the photograph appears to convey, and not in isolation. The Supreme Court further instructed that a more adaptive community standards test must be applied for a continuously evolving society like India.

Under the ***Information Technology Act, 2000, Section 67***of the Act states that publishing obscene content online is punishable with imprisonment of three years and a fine of rupees five lakhs; and subsequent conviction will lead to a punishment of imprisonment of five years and fine of ten lakh rupees. However, under the ***Information technology (Amendment) Act, 2008, section 67(A)*** it has been made clear that a publication of sexual content will lead to a punishment of five years' imprisonment on the first conviction with a fine of rupees ten lakh and a punishment of 7 years with a fine of rupees ten lakh on the subsequent conviction. ***Section 67(B)*** of the amendment which is against child pornography makes it clear that not only publication and viewing but also possession of such pornographic content is punishable with five years' imprisonment and ten lakh rupees on the first conviction and seven years' imprisonment and ten lakh rupees on the subsequent conviction.

1.8 CYBER STALKING

Cyber Stalking has been defined as a crime wherein the stalkers use the internet or any other electronic device to stalk someone. It is an advanced form of stalking which is committed over

[56] *AveekSarkar v State of West Bengal*[2014] 4 SCC257

the online medium.[57] It involves a conduct of harassing or threatening an individual in order to gather information about the victim. Cyber Stalking can be conducted via email, internet and computer. The Internet provides an opportunity for the stalkers to keep a check on the activities of their victims and the risk factor is comparatively less compared to physical stalking as the identity of the stalker can be hidden.

1.9 LEGISLATIVE FRAMEWORK AND POSITION IN INDIA

Cyber Stalking gathered importance after the evolution of the internet. California was the first state to pass the anti-stalking law in 1990. The gravity of cyber stalking came into focus in India with the ***Manish Kathuria Case.***This was first reported case cyber stalking case in India and it was the reason the provisions pertaining to cyber stalking were included in the Information Technology (Amendment) Act, 2008. The Delhi Police arrested Manish Kathuria for stalking a person called RituKohli by illegally chatting with her name on 'www.mirc.com' website. As a result, the victim started receiving obscene calls from various parts of India and abroad. The matter was reported to the Delhi Police wherein a case registered under Section 509 of the Indian Penal Code for outraging the modesty of a women.[58] However, the said section does not cover cyber stalking. This case was an alarm to the Government and as a result ***Section 66A of the Information Technology (Amendment) Act, 2008 i.e., Punishment for sending offensive messages through communication service, etc.***The offences like obscenity, defamation, bullying etc. came under the purview of the said section.

However, the aforesaid section was struck down in the year 2015 in the writ petition ***ShreyaSinghalVs Union of India[59].*** The Apex Court struck down Section 66A of Amendment Act, 2008 as it was misused by the authorities to the effect of violating ***Article 19(1) of the Constitution of Indiai.e., Freedom of Speech and Expression.***

[57]Kabay, M E (2000) Studies and Surveys of Computer Crime, Focus <http://securityportal.com/cover/coverstory2001211.html>

[58] Section 509 of IPC states that, Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both

[59]*ShreyaSinghal v Union of India*WP (Crl) No 167 of 2012

At present, ***Section 72 and Section 72A*** of the Information Technology (Amendment) Act, 2008 regulate cyber stalking. Section 72 of the Act pertains to Penalty for breach of confidentiality and privacy and Section 72A of the Act deals with punishment for disclosure of information in breach of lawful contract.

1.10 PROVISIONS UNDER INDIAN PENAL CODE

There are no direct provisions that deal with the issue of cyber stalking. However, there are certain provisions under the Indian Penal Code that have some linkage with cyber stalking.

a) ***Section 354D defines 'Stalking'***. It states that, any man who,

- follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.

b) ***Section 292 defines 'Obscenity'.*** It states that, the act of sending obscene materials to the victim on a social networking site or through emails or messages etc. or deprave the other person by sending any obscene material using the internet with the intention that the other person would read, see or hear the content of such material, shall amount to the offense under the said section being committed.

c) ***Section 507 relates to 'Criminal Intimidation by anonymous communication'.*** It states that, when the stalker tries to hide his identity so that the victim remains unaware of the source from where the threat comes, it amounts to an offence. This satisfies the very characteristic of cyberstalking i.e., anonymous identity. The stalker shall be guilty if he attempts to conceal his/her identity.

d) ***Section 354C defines 'Voyeurism'.*** It states that, any man who watches, or captures or disseminating the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator.[60]

[60] KPMG (2000) , E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation, USA

1.11 CYBER TERRORISM

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. It is a combination of cyberspace and terrorism. There isn't an appropriate definition for Cyber Terrorism which can be accepted worldwide. However, a universally acknowledged definition of Cyber Terrorism is 'A criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and / or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda'.[61]

1.12 FAMOUS INCIDENTS OF CYBER TERRORISM IN THE WORLD

- ***Attack on the Indian Parliament***

The Indian Parliament was attacked by a cyber-attack on 13th December, 2001. The attackers used new technology and committed forgery to fulfil their end. They forged the gate pass and for the attack they downloaded the official logo of Ministry of Home Affairs, other documents and the layout of the Parliament building. Police found a laptop from main accused Mohammed Afzal and ShaukatHussain Guru. The Police officials established that they have accessed the internet through Pakistan based Internet Service Providers (ISP). Additionally, the Investigating officers found incoming and outgoing cell phone call numbers of deceased terrorists and a satellite connection with deceased terrorist's cell phone.[62]

- ***Yugoslavia Conflict***

[61] Russell G Smith, Peter Grabosky and GrgorUrbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press

[62] SayantanChakravarty, "Parliament attack well-planned operation of Pakistan-backed terror outfits, evidence shows", India Today, December 31st 2001

When NATO[63] air strikes hit the Former Republic of Yugoslavia in Kosovo and Serbia, NATO web servers were subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO's 100 servers were subjected to 'ping saturation', Distributed Denial of Service (DDoS)[64] assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of the American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks caused serious disruption of NATO communications infrastructures.

- ***Epsilon***

Epsilon was one of the costliest cyber-attacks in history. Epsilon was the world's largest provider of marketing and handling services to industry giants such as JP Morgan Chase, Best Buy, and other major financial service providers, retailers and other major companies in 2011. It had an estimated damage cost that ranged from $225 million to $4 billion dollars. Names and email addresses were stolen from Epsilon, the world's largest email marketing firm in 2011, which handled more than 40 billion emails every year, more than 2,000 brands worldwide including Marks and Spencer. The company faced a spear phishing attack, a sophisticated fraud which aims to gather user details by sending emails from a trusted company with many users, such as PayPal. So, in the attack, the hackers targeted the email addresses that they could use for their criminal activities, making the implications a lot greater than estimated.

- ***Sony PlayStation Network, Microsoft's Xbox Live Network Case***

In this case, the confidential data of the employees and their families were leaked in 2014. The company faced a huge loss in revenue due to the publication of employee information which included their salaries, social security numbers, and executive emails. Due to this, an attack was launched by the '*Lizard Squad',* a cyber-terrorist against the Tor Project, a

[63]The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its member states agree to mutual defense in response to an attack by any external party

[64] One common form of DOS and DDOS attacks use a technique known as ping saturation. Ping is a simple Internet utility used to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests

network of virtual tunnels that allow people and groups to improve their privacy and security on the Internet and after that North Korea attacked the network infrastructure wherein the network had gone down for almost 10 hours.

1.13 LEGAL PROVISIONS UNDER THE I.T. ACT

A new ***Section 66F*** was inserted by the Information Technology (Amendment) Act, 2008. Prior to the aforementioned provision, there was no specific provision in the IT Act, 2000 that dealt specifically with Cyber Terrorism.

Section 66F relates to 'Punishment for cyber terrorism'.[65]It stated that,

Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

- denying or cause the denial of access to any person authorized to access computer resource; or
- attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
- introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

- knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer

[65] Section 66F, Information Technology (Amendment) Act, 2008

database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

1.14 IMPORTANT PROVISIONS UNDER THE I.T. ACT, 2000

SECTIONS	OFFENCES	PENALTIES
Section 65	**Tampering with computer source documents**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66	**Hacking the computer system with intent or knowledge**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66B	**Misappropriation of information stolen from computer or any other electronic gadget**	**Imprisonment up to 3 years or fine up to 1 lakh rupees or both.**
Section 66C	**Stealing someone's identity**	**Imprisonment up to 3 years or fine up to 1 lakh rupees**
Section 66D	**Accessing personal data of someone with the help of computer by concealing their identity**	**Imprisonment up to 3 years or fine up to 1 lakh rupees**

Section 66E	**Breach of Privacy**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66F	**Cyber Terrorism**	**Imprisonment which may extend to imprisonment of life.**
Section 67	**Publication of obscene information in e-form**	**Imprisonment up to 5 years and fine up to 1 lakh rupees.**
Section 67A	**Publishing or circulating sex or pornographic information through electronic means**	**Imprisonment up to 7 years or fine up to 10 lakh rupees.**
Section 67B	**Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode**	**Imprisonment up to 5 years or fine up to 10 lakh rupees.**
Section 68	**Failing to comply with the directions of the controller**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 71	**Misrepresentation**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 72	**Breach of confidentiality and privacy**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 72A	**Disclosure of information**	**Imprisonment up to 3 years or fine up to 5**

	in breach of lawful contract	**lakh rupees or both.**
Section 73	**Publishing false digital signature certificate and false in certain particulars**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 74	**Publication for fraudulent purposes**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**

1.15 LET'S SUM UP

In this chapter, we have studied about the varied facets of cybercrimes along with the legislative framework and position in India. We have also seen the provisions under IPC with respect to Cybercrime offences. Finally, we have ended the discussion with the famous incidents of cyber terrorism in the world and the important provisions under I.T. Act, 2000.

1.16 FURTHER READING

- S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81
- Rhiannon Williams, "The Biggest Ever Cyber Attacks and Security Breaches", The Telegraph, Available on http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggestever-cyber-attacks-and-security breaches.html.
- See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

1.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are cybercrimes?

Cybercrimes are illegal acts in which a computer is made a tool or object whereby the means or purpose of committing it involves influencing the function of a compute; or instances involving computer technology wherein unethical or unauthorized behaviour relating to the automatic transmission of data results in creating victims and perpetrators.

2. What are the various facets of cybercrime?

The various facets of cybercrime are as follows:

- Hacking
- Email spoofing
- Trojan attacks
- Salami attacks
- Data diddling
- Intellectual property related crimes
- Phishing and vishing

3. What is cyber pornography?

Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

4. What is cyber stalking?

Cyber Stalking is an advanced form of stalking committed over online medium and can be defined as a crime wherein the stalkers use the internet or any other electronic device to stalk someone.

5. What is cyber terrorism?

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives.

1.18 ACTIVITY

Infer the reason that Information Technology Act is a *'Cyber Crime Friendly Act'*.(1500-2000 words.

Block 2

Digital Signature, Electronic Signature and Laws Related to Certifying Authority of India

Unit 1: Digital and Electronic Signature: Concept and Procedure

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter,you should be able to understand:

- Concept of Public and Private key
- Digital and Electronic signature
- Legal provisions with regard to digital and electronic signature

1.2 INTRODUCTION

Digital signature and electronic signature are used interchangeably but they are not the same. Digital signature is a mere subset of e-signature. Digital signatures are based on asymmetry, or public key, cryptography and are capable of fulfilling the demand of burgeoning e-commerce by not only providing message authentication, integrity and non-repudiation function but also making it highly scalable. Digital Signatures are basically ***'enciphered data'*** created using cryptographic algorithms. It is not a digitalized image of a handwritten signature. Digital signatures are an actual transformation of an electronic message using public key cryptography. It requires a key pair (private key for encryption and public key for decryption) and a hash function (algorithm).[66]

On the other hand, an electronic signature includes all types of electronically approved methods. It could be a graphical stamp, a process or even pressing the 'Agree' button in the terms and conditions etc. It includes simple forms like pressing ***'place order'*** to complex forms like a biometric signature.

1.3 CONCEPT OF PUBLIC AND PRIVATE KEY

Before digitally signing an electronic communication, the sender has to create a public-private key pair. There are two keys used for digital signatures i.e., Private key and Public key.[67] The private key is kept confidential by the signer and used by him only to create the digital signature whereas the public key is more widely known and is used to verify the digital signature by the relying party.

1.4 IMPORTANT TERMS RELATED TO DIGITAL SIGNATURE

"Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature. (Section 2(1) (d) of IT Act, 2000)[68]

[66]The control implications of a public key infrastructure <https://repository.up.ac.za/dspace/bitstream/handle/2263/4067/Bouwer_Control(1999).pdf?sequence=1&isAllowed=y>

[67] Adams, C, [1999] "Understanding Public-key Infrastructure", Macmillan Technical Publishing

[68]Certifying Authorities - Digital Signature Certificates <http://www.digitalsignaturesale.com/certifying-authorities/>

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. (Section 2(1) (f) of IT Act, 2000)

"Certifying Authority" means a person who has been granted a license to issue an electronic signature certificate under Section 24. (Section 2(1) (g) of 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 2(1) (p) of the IT Act, 2000)

"Electronic Signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature. (Section 2(1) (ta) of the IT Act, 2000)[69]

"Electronic Signature Certificate" means an Electronic Signature Certificate issued under Section 35 and includes Digital Signature Certificate. (Section 2(1) (tb) of the IT Act, 2000)

"Key Pair" is an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key. (Section 2(1) (x) of the IT Act, 2000)

"Private Key" means the key of a key pair used to create a digital signature. (Section 2(1) (zc) of the IT Act, 2000)

"Public Key" means the keyof a key pair used to verify a digital signature and listed in the Digital Signature Certificate. (Section 2(1) (zd) of the IT Act, 2000)

1.5 CREATION AND VERIFICATION OF A DIGITAL SIGNATURE

A digital signature is a two-way process, involving two parties, the signer (creator of the digital signature) and the recipient (verifier of the signature). A digital signature is complete, if and only if, the recipient successfully verifies it.[70]

[69] ICAI members use electronic signature for signing audit <https://taxguru.in/chartered-accountant/icai-members-may-use-electronic-signature-signing-audit-reports.html>

- ***Creation of a digital signature***

- The signer demarcates what is to be signed. The delimited information to be signed is termed as the 'message'.
- A hash function[71] in the signer's software computes a hash result (digital fingerprint) unique to the message.
- The signer's software then transforms (encrypts) the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.
- The digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. Since a digital signature is unique to its message, it is useful if it maintains a reliable association with its message.

- ***Verification of a digital signature***

Recipient:

- Receives digital signature and the message
- Applies signer's public key on the digital signature
- Recovers the hash result of the original message by means of the same hash function used by the signer to create the digital signature
- Computes a new hash result of the original message by means of the same hash function used by the signer to create the digital signature
- Compares the hash results recovered[72]

If the hash result computed by the verifier is identical to that of the hash result extracted from the digital signature during the verification process, it indicates that the message remained unaltered and vice versa.

Verification is a two-prong process i.e.,

---

[70]American Bar Association Digital Signature Guidelines <https://horseproject.wiki/index.php/American_Bar_Association_Digital_Signature_Guidelines>

[71] A 'hash result' is used in both creating and verifying a digital signature. It is an algorithm which creates a digital representation or fingerprint in the form of a hash value or hash result of a standard length which is usually much smaller than the message

[72]Top Compelling Reasons Fedena Blog <https://fedena.com/blog/2019/06/top-compelling-reasons-why-your-school-website-must-have-an-ssl-certificate.html>

- to verify whether the signer's private key was used to digitally sign the message and
- to verify whether the newly computed hash result matches the original hash result which was recovered from the digital signature during the verification process.

1.6 DIGITAL SIGNATURE AND PUBLIC KEY INFRASTRUCTURE

The digital signature regime operates online without any human intervention. The Sender sends a digitally signed message and the recipient receives and verifies it. The requirement is that both the sender and the receiver must have the digital signature software at their respective ends. This paves way for the participation of a ***Trusted Third-party (TTP)***to certify the subscriber's identity and their relationship to their public keys. The Trusted Third Party is referred to as a Certifying Authority (CA). The main function of the certifying authority is to verify and authenticate the identity of the subscriber i.e., a person in whose name the digital signature certificate is issued.[73]

A Digital Signature Certificate securely binds the identity of the subscriber. It contains the name of the subscriber, his public key information, name of the certifying authority who issued the certificate, its public key information and the validity of the certificate. These certificates are stored in an online publicly accessible repository maintained by the Controller of certifying authorities or in the repository maintained by the certifying authority. Every Certifying Authority must maintain a repository[74] for the certificates as per the Certification Practice Statement (CPS).

Under the Information Technology Act, 2000, *Section 35 to 40* lay down the procedure for issuance, rejection, suspension and revocation of digital signature certificates. They provide that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000. The fee shall be prescribed by the Central Government and different fees may be prescribed for different classes of applicants. Furthermore, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

[73]Tarek A El-Mageed, Nariman A El-Salam, [2004] "Public Key Cryptosystems and its Applications in Digital Signature" The 2nd International Conference on Informatics and System INFOS2004, Cairo-Egypt

[74] A repository maintains an up-to-date list of all the valid digital signature certificates, and also a list of suspended or revoked certificates

Digital signatures fulfil all statutory requirements associated with the acceptance of handwritten signatures. The law does not recognize the digital signature in a stand-alone environment. It gives recognition to the whole system – the public key infrastructure including the standards, which create and verify digital signatures. Digital signature establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the signer of an electronic message and also confirms that the said signer approved the content of an electronic message.[75]

1.7 PROCESS OF PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure is about the management and regulation of key pairs by allocating duties between contracting parties (certifying authorities/subscribers) laying down the licensing and business norms for certifying authorities and establishing business processes to construct contractual relationships in a digitalized world. The process is as follows:-

- Subscriber applies to Certifying Authority for Digital Signature Certificate.
- The Certifying Authority verifies the identity of the subscriber and issues the digital signature certificate.
- The Certifying Authority forwards the digital signature certificate to the repository maintained by the controller.
- Subscriber digitally signs an electronic message with the private key to ensure sender authenticity, message integrity, and non-repudiation and sends it to the relying party.
- The relying party receives the message, verifies the digital signature with the subscriber's public key and goes to the repository to check the status and validity of the subscriber's certificate.
- Repository does the status check on the subscriber's certificate and reverts back to the relying party.

Under the IT Act, Sections 17 to 34 provide a system for regulation of certifying authorities, to exercise supervision over the activities of certifying authorities and also lay down principles and conditions regulating the certifying authorities.

[75]CH Magazine | VARIOUS AUTHORITIES UNDER THE IT ACT <https://www.chmag.in/articles/legalgyan/various-authorities-under-the-it-act/>

1.8 DIFFERENCE BETWEEN ELECTRONIC AND DIGITAL SIGNATURE

CRITERIA	ELECTRONIC SIGNATURE	DIGITAL SIGNATURE
Definition	**It is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record.[76]**	**It is a term for one technology-specific type of electronic signature.**
Technology	**They can take many forms and can be created by many different technologies. It permits a broad range of 'electronic signatures' to satisfy the requirements of a legal signature.**	**It involves the use of public-key cryptography (asymmetriccryptography) to 'sign' a message.**
Example	**A name typed at the end of an email message by the sender, PIN used in ATM cards to identify the sender to the recipient etc.**	**It is a block of data at the end of an electronic message that attests to the authenticity of the said message. Digital Signatures are a transformation of an electronic message using public-key cryptography.**

[76] Legal Recognition to Electronic records in India <https://scholarticles.wordpress.com/2015/08/27/legal-recognition-to-electronic-records-in-india/>

1.9 LEGAL PROVISIONS RELATED TO DIGITAL AND ELECTRONIC SIGNATURE

The Information Technology Act, 2000 provides a legal framework to authenticate electronic records. The Act facilitates and safeguards electronic transactions in the electronic medium. It is based on UNCITRAL's Model Law on E-commerce, which adopts 'functional equivalent approach' advocating a shift from a paper-based environment to computer-based.[77]

- ***Section 3*** gives legal recognition to electronic records and digital signatures. ***Section 3A*** was inserted by the IT (Amendment) Act, 2008 which in turn allowed electronic signatures to be used for authentication of e-records. Section 3 provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The authentication of the electronic record shall be effected by the use of the asymmetric cryptosystem and hash function which envelops and transform the initial electronic record into another electronic record.
- ***Section 5*** provides for legal recognition of electronic signature. It states, where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.
- ***Section 6*** deals with the use of Electronic Records and Electronic Signature in the context of Government and its agencies.
- ***Section 14*** deals with secure electronic records. It states that, where any security procedure has been applied to an electronic record at a specific point of time, such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
- ***Section 15*** provides for situations when an Electronic Signature can be considered as secure.

[77] Digital Signature | Ministry of Electronics <https://meity.gov.in/content/digital-signature>

- ***Section 16*** provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability, and cost of alternative procedures, the volume of similar transactions entered into by other parties etc.

1.10 ADOPTION OF SECURITY PROCEDURES AND THE IT ACT, 2000

The main purpose of the IT Act, 2000 is to secure electronic records ***(Section 14)*** and secure electronic records ***(Section 15)*** by applying appropriate security procedures.

Section 14 advocates application of any security procedure to make the electronic record secure. A secured electronic record shall be deemed to be a secured electronic record from the time the said security procedure is applied to the time of its verification. It is important to note that the onus of securing an electronic record rests with the creator of the said record. The presumption is that an electronic record is a secured one from the specific point of time when any security procedure has been applied to it to the time of its verification at the recipient's end, till the recipient proves it otherwise.

Section 15 lays down the security features for a subscriber-specific electronic signature, which includes digital signature as well. It provides for 2 specific features:-

- Signature creation data under the exclusive control of signatory or linked to the signatory (the authenticator) and to no other person and
- Storage and affixation of signature creation data as per prescribed processes.[78]

Section 16 of the act enunciates about security procedure. It is proactive in nature as it gives liberty to the Central Government to adopt and assimilate any technology for providing a regime of secure electronic record and electronic signature. This section puts an onus on the Central

[78]Afrianto, Irawan&Heryandi, Andri&Finandhita, Alif&Atin, Sufa. (2019). E-Document Autentification With Digital Signature For Smart City : Reference Model

Government to prescribe the security procedure is having regard to commercial circumstances, nature of transaction and other related factors as it may consider appropriate before adopting such security procedures and practices.[79] The lawmakers have made the Act flexible in terms of technology adoption and assimilation, which would further influence both e-commerce and e-governance transactions. Thedigital payments ecosystem in India has already been revolutionized without even taking cognizance of *Sections 14-16 of the Act.* There are Rules and Regulations pertaining to and for the purpose of regulating the functioning of Certifying Authorities. It lays down procedure and standards (rule 3-8) for securing electronic records and digital signatures. Under ***Rule 3 of the Information Technology (Security Procedure) Rules, 2004***an electronic record shall be deemed to be a secure electronic record for the purpose of the act if it has been authenticated by means of a secure electronic signature.[80]

1.11 LET'S SUM UP

In this chapter, we have studied the concept of public and private key along with the important terms with respect to digital signature. We also saw how a digital signature is created and verified and the difference between digital and electronic signature. Finally, we have ended our discussion with legal provisions pertaining to digital and electronic signature and adoption of security procedures with respect to it.

1.12 FURTHER READING

- https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf
- http://www.ijhssnet.com/journals/Vol_6_No_12_December_2016/7.pdf
- http://www.ijarcs.info/index.php/Ijarcs/article/viewFile/2484/2472

[79] Stamp, M [2011] "Information Security: Principles and Practice" Second Edition, John Wiley and Sons
[80] Banerjee, Arindam (2016) The Impact of Electronic Signatures on Internal Control Systems

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is a digital signature?

Digital signatures are based on asymmetry, or public key, cryptography and are basically *'enciphered data'* created using cryptographic algorithms, and are actual transformations of electronic messages using public-key cryptography.

2. What are the differences between an electronic signature and digital signature?

Electronic signature is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record while a digital signature is a term for one technology-specific type of electronic signature while, digital signatures involve the use of public-key cryptography (asymmetric cryptography) to 'sign' a message.

3. Mention some legal provisions related to the digital and electronic signature?

Some of the legal provisions related to the digital and electronic signature are as follows:

- Section 3 of the Information Technology Act, 2000 which gives legal recognition to electronic records and digital signatures
- Section 5 of the Information Technology Act, 2000 which provides for legal recognition of electronic signature.
- Section 6 of the Information Technology Act, 2000 which deals with the use of Electronic Records and Electronic Signature in the context of Government and its agencies.
- Section 16 of the Information Technology Act, 2000 which provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures.

4. What is public key infrastructure?

Public Key Infrastructure is about the management and regulation of key pairs by allocating duties between contracting parties (certifying authorities/subscribers) laying down the licensing and business norms for certifying authorities and establishing business processes to construct contractual relationships in a digitalized world.

5. How is a digital signature verified?

The verification of a digital signature involves the following steps:

i. Verifying whether the signer's private key was used to digitally sign the message; and
ii. Verifying whether the newly computed hash result matches the original hash result which was recovered from the digital signature during the verification process.

1.14 ACTIVITY

Describe the legal provisions pertaining to digital and electronic signature along with the security procedures in I.T. Act, 2000. (800 words)

Unit 2: Digital Signature Certificate

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of Digital Signature Certificate
- Types and Classes of Digital Signature Certificates
- Certifying Authorities issuing digital signatures
- Advantages and disadvantages of Digital Signature Certificates
- Statutory provisions related to Digital Signature Certificates

1.2 INTRODUCTION

A Digital Signature Certificate is a digital key used to validate and certify the identity of an individual digitally. Such a digital Signature Certificate is issued by a certifying authority. Digital Signature Certificates are created by use of public-key encryptions and form the digital equivalent of physical certificates in electronic format. Digital Signature Certificates form a useful way of signing documents electronically. Similar to physical documents being signed manually, Digital Signature Certificates serve the purpose of digitally signing electronic documents. As per the provisions of the Information Technology Act, 2000, Digital Signature Certificates are considered to be admissible in a court of law.[81] Such Digital Signature Certificates can stay valid for upto a minimum of one year to a maximum of three years. Digital Signature Certificates can be used by both individuals and/or organizations. Digital Signature Certificates function based on MD5 algorithm associated with cryptography, which is, in essence, a 'Message-Digest Algorithm', that receives a message of any length as input and releases as output a 128-bit result which is a 'message digest' based on the input.[82]

Today, India is one of the few nations that have laws associated with Digital Signature Certificates. As per the existing laws, all authorized signatories of organizations and any other professional having the authority to *inter alia* sign documents shall be required to obtain the Digital Signature Certificates. Such group of persons could include but not be limited to directors of companies, auditors or chartered accountants, practising company secretaries or those engaged in jobs, officials working at banks etc. Once the Digital Signature Certificate has been issued and received by the applicant, the certificate can be used by the holder to sign any document online.

1.3 TYPES AND CLASSES OF DIGITAL SIGNATURE CERTIFICATES

There can be four kinds of Digital Signature Certificates, which are as follows:

(a) ***Sign*** – Sign Digital Signature Certificates can be solely used for signing documents. While on one hand, its usage signifies integrity of the data as well as the signer, on the

[81] FeghhiJ and P Williams, Digital Certificates: Applied Internet Security 1st ed Reading, MA: Addison-Wesley [1999]
[82] Stallings W, Cryptography and Network Security, 3rd ed. EnglewoodCliffs, NJ: Prentice-Hall, 2002

other, it ensures that the data does not get altered or tampered. Commonly, Digital Signature Certificates are used with respect to the filing of tax returns.[83]

(b) ***Encrypt*** – Encrypt Digital Signature Certificates can solely be used to encrypt a document, as popularly used by companies to encrypt and upload documents and/or send across classified information. Encrypt Digital Signature Certificates are used in association with e-commerce documents and other documents, legal or otherwise, that are extremely confidential in nature and need extensive protection.

(c) ***Sign and Encrypt*** – Sign and Encrypt Digital Signature Certificates can be used to together serve the individual purposes of each of sign and encrypt Digital Signature Certificates. It helps authenticate information as well as maintain their confidentiality at the same time.

(d) ***Server Certificate*** – These kinds of certificates are used in identifying a server by means of the hoist name and/or IP address that they contain, and are used for ensuring secure communication of data using the internet.

Primarily, there could be three classes of Digital Signature Certificates. They are as follows:

(a) Class 1 Certificate – These Digital Signature Certificates are issued to individuals and/or private users to authenticate the details of the user such as name, email address etc.

(b) Class 2 Certificate – These Digital Signature Certificates can be issued to individuals as well as organizations for both personal as well as professional use. The purpose of its use is to reaffirm and authenticate the details of the signer. It is used most commonly n instances of electronic form filling, income tax filing, registration is done online, email attestation, application for GST etc.

(c) Class 3 Certificate – These Digital Signature Certificates are high assurance certificates that more secure in comparison to Class 2 Certificates, and are arguably considered to be the safest. They provide high safety and security with respect to information and are used mainly in e-commerce and online trading involving privileged information and big amounts of money. Class 3 Digital Signature Certificates are only issued once the holder makes a physical appearance before the certifying authority.[84]

---

[83]Denning, D E Cryptography and Data Security. Reading, MA: Addison-Wesley(1982)

[84] Stallings, W Cryptography and Network Security: Principles and Practice, 4th ed Englewood Cliffs, NJ: Prentice Hall(2006)

*

Class 1	Class 2	Class 3
Certificates are issued to government organizations, business organizations as well as individuals.	**Certificates may be issued to those individuals who belong to business and/or government organizations that are willing to verify the information submitted by such individual subscriber. Certificates can also be issued to organizations that are well-known and are capable of self-verifying the information submitted.[85]**	**Certificates can be issued to both individuals as well as organizations.**
Used to enhance the security associated with personal emails and personal web browsing, and is used primarily to that effect.	**Used for aiding in an organization's administrative and functional needs.**	**Used extensively for e-commerce applications, electronic banking, other online services that rely on online memberships and subscription, etc.**
Assurance provided is of the lowest level in comparison to other kinds of certificates.	**Assurance provided is of more than Class 1 certificates. However, the verification process**	**The validation procedure involved provides assurances stronger than that provided by Class 1**

[85] Practical Security Aspects of Digital Signature Systems: Florian Nentwich, EnginKirda, and Christopher Kruegel Secure Systems Lab, Technical University Vienna(JUNE2006)

	involved with the issuance is more rigorous than that involved in association with Class 3 certificates.	**and Class 2 certificates.**
Certificates help in confirming a user's name and email address.	**A digital certificate signed by the Certifying authority is given to the head of an organization or his/her nominee so that the process of issuing further Certificates can be initiated.**	**Significant assurances associated with the identity of subscribers are provided following the personal physical appearance of such subscribers before the certifying authority.**

While the certifying authority has the right to issue more classes of certificates, it has to be nevertheless ensured that the same be expressly defined along with their purpose as and when issued.[86]

In order for a Class 3 Certificate to be issued, certain requirements that need being fulfilled are as follows:

Individual Applicant	**Company Applicant**	**Government Applicant**
After the application is filled and submitted, the individual applicant will need to be present physically before the Registration Authority with an original copy of one of the following	**An individual representing the company that has subscribed for the certificate has to be present physically before the Registration Authority with proof of ownership and other details**	**An individual representing a government applicant that has subscribed for the certificate has to be present physically before the Registration Authority with a letter on the official letter of the subscriber**

[86]Banday, M Tariq &Dethe, C (2011) Easing PAIN with Digital Signatures. International Journal of Computer Applications

documents : **i) Passport** **ii) Voter ID Card** **iii) PAN Card** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**	**associated with the subscriber company.** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**	**which must contain the following:** i) **Name of the organization** ii) **Administrative department** iii) **Address of the subscriber** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**

1.4 CERTIFYING AUTHORITY

A ***'Certifying Authority'*** is an entity who has been granted the authority of issuing Digital Signature Certificates as per the provisions of section 24 of the Information Technology Act, 2000. All the licensed Certifying Authorities and their contact numbers are available in the public domain.

A Certifying Authority can directly be approached by an applicant with supporting documents of original and self-attested copies for acquiring a Digital Signature Certificate. A Certifying Authority could also be approached for a Digital Signature Certificate also with only the eKYC based authentication details associated with Aadhar Card in which case no supporting documents shall be required. A letter containing the necessary information issued and certified by the bank wherein the applicant of the Digital Signature Certificate holds an account is also considered valid and sufficient for acquiring a Digital Signature Certificate.[87]

[87]Afrianto, Irawan&Heryandi, Andri&Finandhita, Alif&Atin, Sufa. (2019). E-Document Autentification With Digital Signature For Smart City : Reference Model

The applicant of a Digital Signature Certificate holds a private key that corresponds to the public key that is to be listed in the certificate, and further holds a private key which creates the digital signature. The public key which is listed in the Digital Signature Certificate is used to verify the digital signature that the applicant affixes using the secure private key. Once applied, the Certifying Authority could take around three to seven working days for issuing a Digital Signature Certificate.

1.5 UTILITY OF DIGITAL SIGNATURE CERTIFICATES

The utility of Digital Signature Certificateslies in the fact that Digital Signature Certificates can be used as a means of electronic proof of identity of an individual. Digital Signature Certificates can be further used for signing documents digitally or accessing information or availing services over the internet.[88]

Digital Signature Certificates further provide benefits of privacy to their holders and also help authenticate and authorize entities to get involved *inter alia* in electronic transactions.While on one hand Digital Signature Certificates and their usage have been given legal validity owing to the provisions of the Information Technology Act, 2000, on the other, they can also provide a high level of security for online transactions by encrypting information only for the purposes of intended use by the intended recipient(s). The added advantage with respect to Digital Signature Certificates ensures that the information involved remain unaltered in spite of transition.[89]

The major advantages associated with the use and implementation of a Digital Signature Certificate are as follows:

(i) Prevention of Fraud – Use of Digital Signature Certificate eliminates the possibility of fraud by entirely eliminating the scope of alteration therein or creating a duplicate thereof.

(ii) Preserving integrity – Use of Digital Signature Certificates established the validity of a document in all legal, formal and official aspects.

[88]Zheng Y, Imai H and Imai, H (Ed) 2007 Public Key Cryptography, Springer, ISBN: 9783540656449

[89] FIPS (1996) Digital Signature Standard (DSS), FIPS PUB 186-3, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-890, available online at: <http://csrc.nist.gov/publications/fips/fips186-3/fips_186- 3.pdf>

(iii)Advantages in Online Banking – Businesses depending on online banking procedures are extensively benefitted by the use of Digital Signature Certificates.

1.6 INGREDIENTS OF A DIGITAL SIGNATURE CERTIFICATE

The ingredients of a Digital Signature Certificate *inter alia* include the following details:

(a) The name of the individual owing the digital signature certificate
(b) The public key held by the owner of the digital signature certificate
(c) The date of expiry associated with the public key held by the owner
(d) The name of the certifying authority issuing the digital signature certificate
(e) The serial number associated with the digital signature certificate
(f) The digital signature of the owner/user of the digital signature certificate

1.7 SUBSCRIBER'S OBLIGATIONS

Besides imposing statutory obligations on the Certifying Authorities issuing Digital Signatures Certificates, the provisions of the Information Technology Act, 2000 also impose certain obligations on the subscribers applying for the Digital Signature Certificates. Such obligations are as follows:

i) Providing correct information devoid of errors, omissions, misrepresentations etc. in the application for the Digital Signature Certificate.
ii) Accepting the Digital Signature Certificate as generated by the Certifying Authority if all the information contained in the Digital Signature Certificate applied are validated to be true.
iii) In the event there are any changes required to be made in the Digital Signature Certificate of the subscriber to prevent the certificate from being misleading, the same shall be correctly provided by the subscriber forthwith after such change takes place.
iv) Ensuring the protection of the private key in a secure medium.

v) Ensuring that the certificate is terminated in case the information contained in such certificate is inaccurate and misleading.

The Act lists down the duties of subscribers in sections 40, 40A, 41 and 42 in the following manner.[90]

Section 40 *– Generating Key Pair – Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying the security procedure.*

Section 40A *– Duties of subscriber of Electronic Signature Certificate – In respect of Electronic Signature Certificate, the subscriber shall perform such duties as may be prescribed.*

Section 41 *– Acceptance of Digital Signature Certificate – (1) The subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate –*

(a) to one or more persons;

(b) in a repository;

or otherwise demonstrates his approval of the Digital Signature Certificate in any manner;

(2) By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

[90]Ross Anderson and Eli Biham (1996). Tiger: A Fast New Hash Function, Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, pp. 89—97

1.8 DISADVANTAGES OF DIGITAL SIGNATURE CERTIFICATES

In spite of the extensive advantages associated with Digital Signature Certificates, there are a handful of disadvantages that arise from the issuance, use and implementation of Digital Signature Certificates, such as follows:

(a) Financial disadvantage: Certifying Authorities that issue Digital Signature Certificates require a monthly subscription from the applicant of such certificate. Such monthly subscription and the hefty costs involved therewith could become a liability on the entity or individual applying for the Digital Signature Certificate.[91]

(b) Equipment Cost: Electronic signatures that are required to be read by upgraded technology which warrantsthe extensive investment. Such expenses might become too heavy for certain applicants of Digital Signature Certificate.

(c) Deterrence on Clients: Application for and implementation of Digital Signature Certificates involve the use of certain applications and advanced forms of technology. Since the system of issuance and use of Digital Signature Certificate involve an extensive understanding of sophisticated technology and functioning of equipment, some clients might face trouble using Digital Signature Certificate, which could in turn cause deterrence towards using Digital Signature Certificates.[92]

1.9 LET'S SUM UP

In this chapter, we have studied the concept of digital signature certificate along with the types and classes. Furthermore, we also studied about how certifying authority issues the certificate and the obligations of the subscriber. Finally, we have ended our discussion with the advantages

[91]CCA. (2009). Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, CCA India, version 2.4 updated on 14th June 2011
<http://cca.gov.in/rw/resource/dsc _guidelines_r2_4.pdf>
[92] IT ACT (2000), The Information Technology Act, 2000, Government of India
<http://www.mit.gov.in/sites/ upload_files/dit/files/downloads/itact2000/itbill2000.pdf>

and disadvantages of digital signature certificate along with the statutory provisions pertaining to it.

1.10 FURTHER READING

- http://scienceandnature.org/IJEMS-Vol3(2)-Apr2012/IJEMS_V3(2)6.pdf
- Roy, Dr.Abhishek&Karforma, Sunil. (2012). A survey on digital signatures and its applications. JCIT. 3. 45-69.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is a Digital Signature Certificate?

A. A Digital Signature Certificate is the electronic equivalent of physical form of certificates that can act as proof of identity for individuals, or sign documents digitally.

2. Who issues Digital Signature Certificates?

A. An individual or an entity authorised to grant Digital Signature Certificates as per section 24 of the Information Technology Act, 2000.

3. What are the classes of Digital Signature Certificates?

A. Digital Signature Certificates can be classified into three classes – Class 1, Class 2 and Class 3. Class 1 certificates are issued to users to authenticate their details such as name, email address etc. Class 2 certificates verify the identity of a person against a trusted, pre-verified database. Class 3 certificates involve the appearance of the applicant before the certifying authority for proving the identity.

4. How long do Digital Signature Certificates remain valid?

A. Digital Signature Certificates can stay valid for a minimum of one year to a maximum of three years.

5. What is the legal status associated with Digital Signature Certificates?

A. Digital Signature Certificates are admissible in courts of law in accordance with the provisions of the Information Technology Act, 2000.

1.12 ACTIVITY

Describe the issues and challenges associated with addressing identity theft in cyberspace in light of digital signature certificates and their applicability. (800 words)

Unit 3: Regulation and Responsibilitie Certifying Authorities and Controller Certifying Authorities

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Role of Certifying Authorities and Controller of Certifying Authorities
- Regulation of Certifying Authorities and Controller of Certifying Authorities
- Powers of Controllers of Certifying Authorities

1.2 INTRODUCTION

As per the existing laws in our country, Digital Signature Certificates are issued by Certifying Authorities in accordance with the provisions of the Information Technology Act, 2000. Certifying Authorities, therefore, have a very significant role to serve in, which is in turn backed by statutory obligations and responsibilities. Before a Certifying Authority starts issuing Digital Signature Certificates, it is required to receive a license from the controller of certifying authorities. Certifying Authorities, in essence, play a twin role by issuing Digital Signature Certificates to subscribers in one hand and identifying with and authenticating such subscribers

on the other. Given that Certifying Authorities play a very crucial role in the process of generation of Digital Signature Certificates, it is also important to regulate the activities of such Certifying Authorities.

1.3 REGULATION OF CERTIFYING AUTHORITIES

The provisions of the Information Technology Act, 2000 acknowledge an authority superior to Certifying Authorities and refers to the same as the 'Controller of Certifying Authorities'. Chapter VI of the Information Technology Act, 2000 lay down provisions that elaborate upon means and ways for the Controller of Certifying Authorities to regulate Certifying Authorities. Guidelines that are to be followed by Certifying Authorities have also been laid down in ***the Information Technology (Certifying Authorities) Rules, 2000*** and ***the InformationTechnology (Certifying Authorities) Regulations, 2001.***[93]

As per the legal regulations and obligations of the Certifying Authorities, and the powers conferred to them in accordance with the law of the land, the nature of such entity should rather be an administrative authority than being a quasi-judicial body. Accordingly, ***Section 17 of The Information Technology Act, 2000*** lays down those requisites associated with the appointment of the Controller of Certifying authorities and other offices. By virtue thereof, the central government has the authority to appoint the Controller of Certifying Authority which in turn could have three functional departments such as (a) Technology, (b) Finance and Legal and (c) Investigation. Each department is to have a deputy controller and assistant controllers to oversee the smooth functioning of the entity.[94]

As a part of regulating the functions of the Certifying Authorities, the Controller of Certifying Authorities is required to perform certain functions as laid down under section 18 of the Information Technology Act, 2000, which inter alia include:

(i) Exercising supervision over the activities of the Certifying Authorities: As has been stipulated under Rule 31 of the Information Technology (Certifying Authority) Rules, 2000, the Certifying Authority shall be required to conduct half-yearly or quarterly

[93] Information Technology Act, 2000
[94] The Cyber Regulations Tribunal (Procedure) Rules, 2000

audits and submit such reports to the Controller of Certifying Authorities within four (4) weeks from the date of completion of such audit. The essence of this provision lies in the fact that as a Certifying Authority, as a licensee, is required to fulfil such conditions as are stipulated by the Controller of Certifying Authorities.

(ii) Certifying public keys of Certifying Authorities: The Root Certifying Authority of India (RCAI) has been established by the Controller of Certifying Authorities to certify public keys of the Certifying authorities in the country, as a result of which, the RCAI shall be *inter alia* responsible for digitally signing public keys of licensed Certifying Authorities; issuing licenses etc.

(iii) Laying down standards to be maintained by the Certifying Authorities: Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 lays down the standards that are to be considered for the functioning of Certifying Authorities.

(iv) Specifying the qualifications and experience which employees and Certifying Authorities should possess: This provision mandates that a system administrator be appointed to oversee that the protective security measure associated with the system are entirely functional and that a network administrator is appointed as an individual responsible for ensuring that the operations are executed properly.

(v) Specifying conditions subject to which the Certifying Authorities conduct their business.

(vi) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of an Electronic Signature Certificate and the public key.[95]

(vii) Specifying the form and content of an Electronic Signature Certificate and the key.

(viii) Specifying the form and manner in which accounts shall be maintained by Certifying Authorities: as per regulation 3 (vi) of the Information Technology (Certifying Authorities) Regulations, 2001, Certifying Authorities are required to comply with the financial mandates and parameters as issued under the Act during the period when the license will stay valid.

(ix) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them: This is to be complied with in sync with Rule 31 and

[95] Gupta, Apar, Commentary on Information Technology Act, 2000, LexisNexis ButterworthsWadhwaNagpur Publication, Ed. 2, 2011

32 of the Information Technology (Certifying Authorities) Rules, 2000, which in turn lay down the terms of regulating audit and auditor's relationship with Certifying Authorities.

(x) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of systems: As per Rule 19(2) of the Information Technology (Certifying Authorities) Rules, 2000, security guidelines have been laid down to ensure that integrity, confidentiality and availability of data, services and systems of Certifying Authorities are maintained.

(xi) Specifying the manner in which the Certifying Authorities shall conduct dealings with the subscribers: As per regulation 3 of the Information Technology (Certifying Authorities) Rules, 2001, a Certifying Authority is required to use methods which the Controller of Certifying Authorities has approved for the purposes of verifying a subscriber's identity before issuing or renewing any public key.[96]

(xii) Resolving ant conflict of interests between the Certifying Authorities and subscribers: As per Rule 12 of the Information Technology (Certifying Authorities) Rules, 2000, disputes arising between Certifying authorities and subscribers shall be referred for resolution to the Controller of Certifying authorities through arbitration or any other mode of resolution.

(xiii) Laying down the duties of the Certifying Authorities.

(xiv) Maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public: Rule 22 of the Information Technology (Certifying Authorities) Rules, 2000 makes reference to the database of Certifying Authorities, thereby stating that the Controller shall be required to maintain a database for the disclosure record.

1.4 STATUTORY RESPONSIBILITIES OF CERTIFYING AUTHORITIES

The statutory responsibilities and obligations that Certifying Authorities are legally required to abide by have been laid down in the provisions of the Information Technology Act, 2000:

(a) ***Section 35*** – Certifying Authority to issue Electronic Signature Certificate: This provision addresses that any person who wants to acquire a Digital Signature Certificate

[96] Henery Chan, Raymond Lee, Thoram Dillon, Elizabeth Chang, E-Commerce; Fundamentals and Applications, Wiely IndiaPvt. Ltd (India), Reprint 2008

can file an application addressing the Certifying Authority requesting the issuance of the certificate in the prescribed manner, coupled with the payment of the requisite application fee which shall not exceed Rs. 25,000/- (Rupees Twenty-Five Thousand only). The provision further mandates for the application to be accompanied by a 'certification practice statement' or any other statement specifying the necessary particulars, in absence of the former. In approval of the application submitted, a Digital Signature Certificate may be issued by the Certifying Authority after making the necessary enquiries, or the application may be rejected with relevant reasons recorded in writing after providing the applicant with an opportunity of showing cause against such rejection of the application.[97]

(b)***Section 36*** – Representations upon issuance of Digital Signature Certificate: The provision lists down the requisites that a Certifying Authority is legally required to ensure while issuing a Digital Signature Certificate. It is mandated as per the section that –

i. The provisions of the Act, as well as the rules and regulations associated with it, have been complied with while the issuance of the Digital Signature Certificate;
ii. The Digital Signature Certificate has been published or otherwise made available to the applicant and that the applicant has acknowledged the same;
iii. The applicant holds the private key and its corresponding public key as listed in the Digital Signature Certificate;
iv. The applicant holds the private key that creates a digital signature;
v. The public key as listed in the Digital Signature Certificate is capable of verifying the digital signature affixed by the private key that the applicant holds;
vi. The public key and the private key held by the applicant together form a valid and functioning key pair;
vii. The Digital Signature Certificate only contains information that is accurate;
viii. No material fact exists that is potentially capable of adversely affecting the reliability of the aforementioned conditions.[98]

[97] Sharma, Vakul, Information Technology and Practice, Universal Law Publication, 2008
[98] Indira Carr, India joins the cyber-race: Information Technology Act 2000, Int. TJs 2000, 6(4), 122-130, (2000)

(c)***Section 37*** – Suspension of Digital Signature Certificate: this provision of the act endows upon the Certifying Authority issuing the Digital Signature Certificate the power to suspend such Digital Signature Certificate granted on certain grounds; such as, upon receipt of a request of such suspension of certificate from the person listed as the subscriber in the Digital Signature Certificate or any other person authorised to act on his or her behalf; or in the event the Certifying Authority believes that the suspension of such Digital Signature Certificate shall be in the interest of the public at large. Furthermore, the provision further lays down that unless the subscriber has been given an opportunity of being heard with respect to such suspension of the Digital Signature Certificate, the certificate shall not be suspended for any longer than fifteen days. It further imposes on the Certifying Authority the obligation of communicating to the subscriber all information associated with such suspension of the Digital Signature Certificate.

(d)***Section 38*** – Revocation of Digital Signature Certificate: This provision addresses instances that could cause the Certifying Authority issuing a Digital Signature Certificate to revoke it. The circumstances in which the Certifying Authority could so revoke a Digital Signature Certificate granted by itself are –

(i) The subscriber of the Digital Signature Certificate making a request of revocation of the certificate granted;

(ii) A person duly authorised by the subscriber of the Digital Signature Certificate making a request of revocation of the certificate granted;

(iii) Upon death or insolvency of the subscriber of the Digital Signature Certificate;

(iv) In instances wherein the subscriber of the Digital Signature Certificate is a firm or a company, the respective dissolution and winding up thereof;

(v) In the event the Certifying Authority issuing the Digital Signature Certificate is of the opinion that incorrect and erroneous information has been represented as material facts in the Digital Signature Certificate;

(vi) In the event the Certifying Authority issuing the Digital Signature Certificate is of the opinion that a material requirement associated with the issuance of the Digital Signature Certificate remains unfulfilled;

(vii) In the event, the Certifying Authority issuing the Digital Signature Certificate is of the opinion that the security system and/or the private key held by the Certifying Authority had been compromised so as to affect the reliability of the Digital Signature Certificate.

The provision, however, emphasises on how the Digital Signature Certificateis not to be revoked without giving its subscriber a reasonable opportunity of being heard. It further imposes on the Certifying Authority the obligation of communicating to the subscriber all information associated with such revocation of the Digital Signature Certificate.[99]

1.5 STATUTORY POWERS OF CONTROLLERS OF CERTIFYING AUTHORITIES

The Information Technology Act, 2000 lays down provisions to address the powers of the Controller of Certifying Authorities in a manner such as follows:

(i) ***Section 27*** – Power to delegate – As per the Act, the Controller shall have the power to authorize the deputy controller of Certifying Authorities, or any other office, in writing, to exercise the powers of the Controller in the same capacity. This provision of the Act is to be ideally read with section 17 thereof, which in turn lays down the organizational structure of the Controller and its team along with the Deputy Controllers, Assistant Controllers and other officers and employees. Nevertheless, in spite of such delegation made by the Controller, the quasi-judicial powers held by the Controller to resolve disputes, if any, between the Certifying Authorities and the subscribers, shall necessarily be retained with the Controller.

(ii) ***Section 28*** – Power to investigate contraventions- Any contravention of the provisions of the Act and/or rules and/or regulations can be taken up for investigation by the Controller or any officer authorized by the Controller. In such event of an investigation, the powers conferred on Income Tax authorities under chapter XIII of the Income Tax Act, 1961, shall apply on the Controller or any other officer authorized by the Controller for the purposes of this provision, however, in accordance with the limitations as laid down under that Act. This power as grated vide this provision is solely investigative in nature. This provision further signifies

[99]Vakul Sharma, Information technology: Law and Practice, Universal Law Publication, Ed. 2, 2008

that the Controller or any other officer authorised by him/her, shall be deemed to have the power to impound and retain in custody documents or books of accounts produced through search or seizure for such period of time that it may deem fit.

(iii)***Section 29*** – Access to computers and data – This provision grants to the Controller or any other person authorized by it broad powers to search and have access to any computer system, apparatus, data connected to such system, etc. solely based upon the reasonable cause to believe that a contravention of the Act or its provisions has been committed.

1.6 CONCLUSION

The provisions of the Information Technology Act, 2000 address the necessity of ensuring that the integrity associated with the system of acquiring and implementing digital signatures is maintained through the delegation of responsibilities amongst various statutory bodies such as Certifying Authorities, Controller of Certifying Authorities, etc. In a world which is going through a dramatic transition that envisages a sea of technological changes which might take extensive sophistication to tackle, it is of utmost importance to ensure that there is due regulation at every stage of action, and that requisite measures have been taken to address any mishap and/or contravention of the ideal provisions laid down as guidelines. In an age where digital signatures are replacing manual signatures, and digital signature certificates are gaining prominence; and public at large are slowly and steadily acknowledging the convenience associated with such change, it is essential that the government ensures that there is enough regulation in place to address instances wherein a misuse or misinterpretation of such nascent and modern technology could take place.[100] It is for this purpose that the Certifying Authorities have been statutorily established, and the Controller of Certifying Authorities have been laid down. Furthermore, the law of the land also ensures that there are specific guidelines established to address the functioning of such authoritative bodies, establish their hierarchy, carve out their responsibilities and powers and in turn create inter-linking of laws for better implementation of such provisions. It is therefore extremely important to learn about the responsibilities, functions and modes of regulating Certifying Authorities as well as Controllers of Certifying Authorities.

[100]VivekSood, Cyber Law Simlpified, Fourth Ed., 2008, Tata McGraw-Hill Publishing Company Ltd

1.7 LET'S SUM UP

In this chapter, we have studied who is a certifying authority along with the regulations and statutory powers under the Information Technology Act, 2000. Finally, we have ended the discussion with the powers given to the certifying authorities.

1.8 FURTHER READING

- http://www.commonlii.org/sg/journals/SGJlIntCompLaw/2003/9.pdf
- Regulation of Certifying Authorities - The Informational Tech. Act, 2008, B.Com, EDUREV.IN (2019), https://edurev.in/studytube/Regulation-of-Certifying-Authorities-The-Informati/74d7d226-f41e-4dfa-97e8-4a9b6bf40993_p?courseId=-1 (last visited Nov 19, 2019).
- Ikram, N. & A., Mahboob,. (2002). Regulatory Issues with Certification Authorities.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Who is a Controller of Certifying Authorities?**

A. A Controller of Certifying Authorities is the entity that supervises the functioning of the Certifying Authorities.

2. **What are the functions of the Controller of Certifying Authorities?**

A. The functions of the Controller of Certifying Authorities inter alia include supervising the functions of the Certifying Authorities, certifying public keys for Certifying Authorities, laying down standards to be maintained and followed by Certifying Authorities etc.

3. **What are the statutory powers of Controller of Certifying Authorities under the existing laws?**

A. The statutory powers of Controller of Certifying Authorities under the existing laws include the power to delegate, the power to investigate contravention of provisions of the act, access to computer data, etc.

4. Which provisions of the Act address the statutory responsibilities of certifying authorities?

A. The provisions of the Act address the statutory responsibilities of certifying authorities are sections 35, section 36, section 37 and section 38.

5. What are the sources of laws, rules and regulations that address the functioning and regulation of Certifying Authorities and Controller of Certifying Authorities?

A. The sources of laws, rules and regulations that address the functioning and regulation of Certifying Authorities and Controller of Certifying Authorities are provisions of the Information Technology Act, 2000, Information Technology (Certifying Authorities) Rules, 2000 and the Information Technology (Certifying Authorities) Regulations, 2001.

1.10 ACTIVITY

Under the IT Act 2000, what are the implications for 'Certifying Authorities'? (800-1000 words)

Unit 4: Addressing Offences: Penalties and Compensation

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Concept of Offences in Cyber Laws
- Commission of Offenses owing to Acts and Omissions of the Controller
- Commission of Offenses owing to Acts and Omissions of the Controller of Certifying Authorities

1.2 INTRODUCTION

The interesting aspect relating to penalties associated with cyber laws is that the provisions addressing them are directed towards penalties towards damage to computer and computer systems as well as towards the process of adjudication. For example, while on one hand, the provisions of the Information Technology Act, 2000 address issues of breach of security or privacy, on the other, it also deals with acts of failing to protect data and privacy. Similarly, the provisions of the Act further address instances wherein the Controller of a Certifying Authority has acted in a manner that is in violation of the provisions of the Act, or had omitted performing

its duties and responsibilities so as to contravene the provisions of the Act. The provisions of the Act and the rules and regulations pertaining to penalties, compensation and adjudication hence have to be read in sync with the essence of cyber laws at large. The Act is governed by the principle **"*He who does not prevent a crime when he can, encourages it.*"**

1.3 PROVISIONS APPLICABLE TO CERTIFYING AUTHORITIES AND THEIR CONTROLLER

The Information Technology Act, 2000 lays down provisions that give the Controller of Certifying Authorities the power to direct certain necessary measures to be taken to ensure compliance with the provisions of the Act; and any violation by any individual of such direction or order as given by the Controller is deemed to constitute an offence under the Act.

Similarly, suppression of material facts and/or misrepresentation of facts from Certifying Authorities or their Controller for the purposes of obtaining a license or an electronic piece of document is an offence in accordance with the provisions of the Act.[101]

An elaborate understanding with respect to the aforementioned provisions are provided hereinbelow:

i) ***Section 68 – Power of controller to give directions*** *– (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder. (2) Any person who intentionally and knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction or imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both.*[102]

This provision is in turn backed by the ***'Information Technology Security Guidelines'*** and the ***'Security Guidelines for Certifying Authorities'*** issued under the Information Technology (Certifying Authorities) Rules, 2000 which prescribe the security standards which are to be

[101] Offences & Penalties under the IT Act, 2000 <http://www.legalservicesindia.com/article/439/Offences-&-Penalties-under-the-IT-Act,-2000.html>

[102] The Information Technology Act, 2000, s 68(2)

observed by Certifying Authorities and endowing upon them the power to issue directions. While a general interpretation of the provision makes it is evident that the Controller has the power to Certifying Authorities and/or employees thereof, in essence such power can be further extended to apply on subscribers of a digital certificate as well, which can be inferred by a combined reading of ***section 68 with section 18(1) of the Information Technology Act, 2000,*** which states that the Controller shall expressly have the power to resolve any and all conflicts of interests and/or disputes between the subscriber and the respective Certifying Authorities.

Sub-section (2) of the provision goes on to establish that the offence committed by way of non-compliance of the order passed under sub-section (1) shall be a cognizable and non-bailable offence. Since section 27 of the Act allows a Controller to delegate its authorities and responsibilities to a Deputy Controller or an Assistant Controller; accordingly, a non-compliance of the Controller's order by such Deputy Controller or the Assistant Controller shall also fall within the ambit of section 68.

A combined reading of section 68 of the Act with sections 28 and 29 which in turn expressly grant to a Controller the power to investigate contraventions of the Act will clarify that the Certifying Authority has the responsibility to ensure that there is no contravention of the Act in the first place; and of at all the same is conducted by any entity and/or individual, then it will constitute as an offence.

ii) ***Section 71*** *– Penalty for misrepresentation – whoever makes any misrepresentation to or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both.*

In addition to the powers already endowed upon the Certifying Authorities and their Controller through ***section 25 and section 38 of the Act*** to suspend and revoke the license and digital signature certificates, this provision additionally bestows upon the Certifying Authority as well as its Controller the obligation to ensure that applicants who misrepresent information or suppress material information are brought within the ambit of criminal charges.

These two aforementioned provisions of the Act bring to the fore how the intention of the legislature was to address such instances in a criminal light wherein any entity, whether statutory

or otherwise, associated with electronic transactions and/or applications and/or involved any correspondence involving the cyberspace tries to misuse the relevant provisions of law and take advantage thereof.

1.4 PENALTIES IN RESPECT OF DAMAGE TO SYSTEMS ASSOCIATED WITH CYBERSPACE

The Information Technology Act, 2000 addresses instances of cyber contraventions through provisions that deal with penalties and/or compensation. Majorly section 43 to section 45 address the aforesaid and in turn list down variable penalties applicable to the respective offenders in accordance with the nature of offence committed.[103] A brief overview of the provisions is provided hereinbelow:

a) ***Section 43*** lists the various instances wherein there could be damage caused to computers or their systems or networks.
b) ***Section 43 A*** deals with an act of failure to protect sensitive data and entails payment of damages by the contravener by way of compensation.
c) ***Section 44*** directs for a penalty to be provided for failure in furnishing information by any person who is required by the Act to provide such information or file any return or maintain books of accounts.
d) ***Section 45*** addresses residuary penalty towards those who violates the rules and regulations made in association with the Act and for the specific contravention of which no penalty has separately been provided.

Section 43 lays down that unauthorized access to computers, an attempt thereof or an assistance thereto are offences under the Act. The ambit of the clause states that such unauthorized access shall cover both physical and virtual access to the computer or its system or network. Such access may be established inter alia if the computer is found to have performed a function as a result of such access. The provision further addresses unauthorized infringement of digital data stored in such computer or its network inter alia through downloading, copying, extracting etc. For the purposes of this provision, downloading, copying and extracting may be differentiated in the following manner –

[103]Penalties and Adjudication in IT ACT 2000
<https://www.pathlegal.in/Penalties-and-Adjudication-in-IT-ACT-2000-blog-1831947>

Downloading	***Copying***	***Extracting***
A file containing digital content being retrieved from a remote computer or network.	A file containing digital content being retrieved from a remote computer or network and then being saved in a storage medium.	A file containing digital content being retrieved from a remote computer or network and then being selectively extracted.

The provision further addresses instances wherein contaminants may be introduced within the computer or its network, and any other attempts that can potentially be made to contaminate data contained in a computer or its network, or destroy, steal, delete, alter the same. Such unauthorized damage to the contents contained in the computer or its computer could be both physical as well as virtual. For the purposes of this provision, physical unauthorized damage and virtual unauthorized damage may be differentiated in the following manner:[104]

Physical Unauthorized Damage	***Virtual Unauthorized Damage***
This could imply changing the configuration of the original software or the original hardware of any computer, computer system or computer network and/or destroying, deleting, altering, modifying in any manner whatsoever the binary files (which shall include but nit be limited to data or other computer programs) available in a computer, computer system or computer network in an unauthorized manner.	This could imply changing the configuration of the original software or the original hardware of any computer, computer system or computer network and/or destroying, deleting, altering, modifying in any manner whatsoever the binary files (which shall include but nit be limited to data or other computer programs) available in a computer, computer system or computer network in an unauthorized manner by way of being remotely connected to such device or network using

[104]Damages or Compensation under IT Act 2000 in India <https://cybercrimelawyer.wordpress.com/2018/04/12/damages-or-compensation-under-it-act-2000-in-india/>

	satellite and/or terrestrial waves and/or microwaves and/or other communication media.

Disruption of a computer or its system or network or denial of access thereto is also considered an offence under this provision. A summary of the sub sections of Section 43 of the Act along with the scope thereof is provided hereunder:

Information Technology Act, 2000	***Scope of Section 43***
Section 43 – Penalty and compensation for damage to computer, computer system, etc. : If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network[105]	The provision majorly addresses all the probable contraventions arising out of unauthorized access to computer, computer system or computer network.
(a) Accesses or secures access to such computer, computer system or computer network or computer resources;	Instances of cracking, hacking, data theft, software piracy etc. will be addressed as a part hereof.
(b) Downloads, copies or extracts data, computer database or information from such computer, computer system or computer network, including information or data stored or held in any removable storage medium;	Instances of digital copying, data theft, violation of privacy will get addressed.

[105]ISACA *State of Cybersecurity: Implications for 2015*
<http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf>

(c) Introduces or causes to be introduced any contaminant or computer virus into any computer, computer system or computer network;	Instances of deletion, alteration, destruction, modification of any data stored in a computer would get addressed.
(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;	Instances related to forgery, online fraud, violation of privacy would get addressed.
(e) Disrupts or causes disruption of any computer, computer system or computer network;	Instances such as spamming attacks, denial of service etc. will get addressed.
(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;	Issues related to system interference, misuse of computer devices etc. get covered hereunder.
(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of the Act, rules or regulations made thereunder	Instances of illegal access, misuse of computer devices etc. get covered hereunder.

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network	Online fraud, phishing, identify theft etc. are the instances that could be addressed through this provision.
(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means	Cracking, hacking, data theft, interference into and loss of data, online frauds and forgeries etc. are instances to get covered under this sub-section.
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage	This sub-section could cover instances related to violations of computer programs and software, theft, piracy etc.

Section 43A addresses all instances of violation of the Act arising and accruing from negligence on part of the data processor or controller. This provision is proactive in nature and aims at protecting personal data and information. The provision further identifies body corporates as 'data processors and controllers for possessing, dealing with and/or handling sensitive data, as the case may be. As opposed to the provisions of section 43, section 43A is specifically addressed towards body corporates. The provision further goes on to warrant that in the event

there is a violation of such sensitive and/or personal data invoking the contents of this section, such violation shall entail payment of compensation.[106]

Section 44 of the Act addresses a range of offences thereby imposing a range of penalties on the contravener of such provision in the following manner:

Section 44	***Authority***	***Applicability***	***Penalty Amount***
Clause (a)	Controller or the Certifying Authority	Subscribers, Auditors, Computer Resource Incharge, etc.	Not exceeding Rs. 1,50,000/- (Rupees One Lakh and Fifty Thousand only) for each such failure.
Clause (b)	Controller, any government agency, statutory authority	Subscribers, Auditors, Computer Resource Incharge, etc.	Not exceeding Rs. 5,000/- (Rupees Five Thousand only) for each day during such continuing failure.
Clause (c)	Controller, any government agency, statutory authority	Certifying Authority, Computer Resource Incharge, etc.	Not exceeding Rs. 10,000/- (Rupees Ten Thousand only) for each day during such continuing failure

Section 45 is in essence effective against all contraventions for which no separate penalty has been provided.[107] Therefore, unless an offence is carefully judged and categorized under sections

[106]National Institute of Standards Technology*Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments*.
<http://dx.doi.org/10.6028/NIST.SP.800-30r1>

43, 43A or 44, it will by default invoke section 45. A summary of the penalties associated with the provisions is provided hereunder:[108]

Contraventions under the Act	***Penalty Amount***
Section 43 – Penalty and compensation for damage to computers and computer systems	i) Less than Rs. 5,00,00,000/- (Rupees Five Crores only) before the adjudicating officer ii) More than Rs. 5,00,00,000/- (Rupees Five Crores only) before the competent civil court.
Section 44 – Penalty for failure to furnish information, return, etc.	i) Less than Rs. 1,50,000/- (Rupees One Lakh and Fifty Thousand only) for each such failure. ii) Not exceeding Rs. 5,000/- (Rupees Five Thousand only) for each day during such continuing failure. iii) Not exceeding Rs. 10,000/- (Rupees Ten Thousand only) for each day during such continuing failure
Section 45 – Residuary Penalty	Not exceeding Rs. 25,000/- (Rupees Twenty Five Thousand only).

1.5 LET'S SUM UP

In this chapter, we have studied the concept of offences in cyber law along with those provisions that are applicable to Certifying Authorities and their Controller. Finally, we have ended the discussion with the penalties in respect of damage to systems associated with cyberspace.

[107]<http://www.meity.gov.in/content/information-technology-act-2000>
[108] The Gazette of India, The Information and Technology Act, 2000, no. 27 of 2000, The Ministry of Law, Justice and Company Affairs, Part II, New Delhi

1.6 FURTHER READING

- Zenithresearch.org.in (2019), http://zenithresearch.org.in/images/stories/pdf/2012/May/ZIJBEMR/13_ZIBEMR_VOL2_ISSUE5_MAY2012.pdf (last visited Nov 22, 2019).
- Indian - Computer Emergency Response Team, Cert-in.org.in (2019), https://www.cert-in.org.in (last visited Nov 22, 2019).

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the powers of the controller to give directions?**

As per Section 68 of the Act, The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder. (2) Any person who intentionally and knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction or imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both.

2. **What is the punishment for misrepresentation?**

As per Section 71 of the Act, whoever makes any misrepresentation to or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both.

3. **Give a brief overview of the provisions with respect to damages to systems associated with cyberspace?**

a) Section 43 lists the various instances wherein there could be damage caused to computers or their systems or networks.

b) Section 43 A deals with an act of failure to protect sensitive data and entails payment of damages by the contravener by way of compensation.

c) Section 44 directs for a penalty to be provided for failure in furnishing information by any person who is required by the Act to provide such information or file any return or maintain books of accounts.

d) Section 45 addresses residuary penalty towards those who violates the rules and regulations made in association with the Act and for the specific contravention of which no penalty has separately been provided.

1.7 ACTIVITY

Discuss the powers of the investigating machinery under the Information Technology Act, 2000. (1000 words)

Block 3
Laws related to E-Service Delivery and Service Providers

Unit 1: E-Services Delivery Laws in India

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- E-Service Delivery Concept in India
- Purpose of the Electronic Delivery of Services Bill (EDS), 2011
- Functions and Powers of Director of Electronic Service Delivery.

1.2 INTRODUCTION

Government of India has been at the forefront of using technology in different aspects of governance, be it satellite-based communication in the 1980s or use of electronic messaging much before the origin of the internet in the country or even the use of video conference for monitoring of government programme and schemes across the country. National Informatics Centre, an attached office of Ministry of Electronics & IT has been closely working with the government in provisioning state-of-the-art infrastructure in the form of nationwide network

(NICNET), data centres and video conferencing facilities to name a few. Digital technologies are vital for the inclusive growth for a country like India, which is at the peak of its demographic dividend.

The story of India's digital transformation is one of an ***Information and Communications Technology (ICT)*** led development by use of technology that is affordable, inclusive and transformative. By ensuring digital access, digital inclusion and digital empowerment, the ***'Digital India'*** programme[109] have brought digital technologies a positive change towards good governance that is easy, economical, transparent and efficient in governance. Digital delivery of services to citizens forms the driving force for the next generation growth and knowledge-based economy. India is now poised for the next phase of growth - the creation of tremendous economic value and empowerment for citizens as a new digital application sector.

Digital India has given boost to entrepreneurship and has enhanced access to health, education and public utilities. It has led India to revolutionize governance by delivering speedy and transparent services to citizens, ensuring their participation and empowering them with the conducive environment to connect and grow.

1.3 ELECTRONIC DELIVERY OF SERVICES BILL INTRODUCED IN PARLIAMENT OF INDIA

The Electronic Delivery of Services Bill (EDS), 2011, aimed at bringing transparency in public dealings and checking corruption, was tabled in Parliament. The Bill seeks to reduce the interface between public and government officials to save time and costs as people will get access to documents like driving license and other permits online. The EDS Bill allows for ***"delivery of public services through electronic mode including the receipt of forms and applications, issue or grant of license, permit, certificate, sanction or approval and the receipt and payment of money."*** Centre, as well as the states, will have to deliver the said public services electronically within five years of the commencement of the Act. The period may be extended for a further period of up to three years in consultation with the Central Commission or the State Commission, the Bill said.

[109]'E-Governance In India : Empowering Citizens - Current Affair Article For UPSC, IAS, Civil Services And State PCS Examinations | Dhyeya IAS Best Coaching For UPSC, IAS,Civil Services, State PSC/PCS Exam' (*Dhyeyaias.com*, 2020) <https://www.dhyeyaias.com/current-affairs/perfect-7-magazine/e-governance-in-india>

"Every competent authority shall publish within 180 days from the commencement of the Act, the list of all public services to be delivered through electronic mode," it added. The Bill requires each Ministry or Department to identify the basket of citizen-centric services to be delivered through the electronic means along with the delivery channels, with stipulated timelines and service levels for each service. An aggrieved person may file a complaint under the Grievance RedressalMechanism, the Bill imposes penalties of up to Rs 5,000 for officials in case they fail to adhere to the norms.

In case of persistent default, the penalty may extend up to Rs20,000, the Bill said The Bill also envisages setting up a Central Electronic Service Delivery Commission and a State Electronic Service Delivery Commission to monitor the implementation of the Act on a regular basis. Any person aggrieved by the order of the Grievance Redressal Mechanism may make a representation to the Central Electronic Service Delivery Commission or the State Commission as the case maybe, the Bill said.

A bill to provide for delivery of public services by the Government to all persons by electronic mode to enhance transparency, efficiency, accountability, accessibility and reliability in the delivery of such services, and including matters connected therewith or incidental thereto. WHEREAS it is considered necessary to provide a legal framework to promote efficient electronic delivery of government services, 2011.[110]

1.4 DUTY OF THE COMPETENT AUTHORITY TO NOTIFY THE LIST OF PUBLIC SERVICES TO BE DELIVERED THROUGH ELECTRONIC MODE

(1) Every Competent Authority shall notify within a period of thirty days from the coming into force of these rules-

(a) The public services of the department, agency or body, which can be delivered through electronic mode;

[110]THE ELECTRONIC SERVICE DELIVERY BILL, 2011 <https://www.prsindia.org/uploads/media/draft/Draft%20Electronic%20Service%20Delivery%20Bill-2011.pdf>

(b) The date by which each such service shall be made available through electronic mode,

(c) Lay down norms for efficiency, quality and accuracy in the form of service levels; and

(d) The designated officers for delivery of each such service through electronic mode.

(2) Notwithstanding anything stated above, all public services shall be delivered in electronic mode within 5 years from the commencement of this Bill; Provided that this period may, for reasons to be recorded, be extended for a further period not exceeding 3 years by the appropriate Government; Provided further that if it is not feasible to render a public service through electronic mode, then the appropriate government shall issue a notification to that effect.

(3) The competent authority, while introducing electronic services, shall ensure that

a) The processes and forms relating to such services are simplified initially and periodically thereafter; and
b) Assisted access to such electronic services is also made available.

(4) The Central Government may, from time to time, prescribe electronic governance standards as may be necessary for ensuring interoperability and security.[111]

1.5 FUNCTIONS AND POWERS OF DIRECTOR OF ELECTRONIC SERVICE DELIVERY

The Director of Electronic Service Delivery shall discharge the following functions and powers, namely:-

a. To authorise, suspend or terminate the services of the Authorized Service Providers;

[111](Environment.delhigovt.nic.in, 2020) <http://environment.delhigovt.nic.in/wps/wcm/connect/29bf44804dd72a98a833ec8291a3c3a2/ESD+Rules.pdf?MOD=AJPERES&lmod=-1976042643>

b. To determine norms relating to the selection of authorised agents by the authorised Service Providers and authorised agents;[112]
c. To determine functions, responsibilities and liabilities of authorised Service Providers and authorised agents;
d. To determine norms on the service levels to be complied with by the authorised Service Providers and authorised agents;
e. To determine service charges be charged by the authorised Service Providers and authorised agents for providing e-services;
f. To determine terms and conditions relating to the authorisation, suspension or termination of the services of the authorised Service Providers and authorised agents; and
g. To make alternative arrangements for delivery of e-services, in case of such suspension or termination of services of authorised Service Providers and authorised agents.

- Director of Electronics Service delivery may delegate any of his power to any official of Government of NCT of Delhi or Autonomous Body/Local Body of Government of NCT of Delhi through an administrative order.

- ***Authorised Service Providers for Electronic Service Delivery***- The Authorised Service Provider shall provide the notified public services electronically to the users in conformity with these rules, by establishing appropriate delivery infrastructure and a network of authorised agents, as determined by the Director of Electronic Service Delivery.

- ***Appointment of authorised agents by the authorised Service Provider***-
  The authorised Service Provider may appoint such number of authorised Agents, as may be required to deliver the services electronically to fulfil the norms of efficiency, quality and accuracy laid down by the Competent Authority.[113]

[112] Das, Sudhir Chandra. (2012). E-Governance Mechanism in India: Experiences from Selected E-Governance Projects. Mirror: Peer Referred Bi-annual Research Journal of Commerce, Management and Social Science, Kerala INDIA II 166-177

- The authorised Service Provider shall ensure that he as well as all the authorised agents obtain Digital Signature Certificates before they commence operations for delivery of public service electronically.

- The authorised Service Provider may also impart appropriate training to the authorised agent to impart them the skills required to deliver the electronic services efficiently and in an error-free manner.[114]

- ***Commencement of operations by Authorised Service Provider-***
  The Authorised Service Provider shall commence its commercial operation for Electronic Service Delivery only after –

  - He has confirmed in writing or through e-mail duly signed by digital signature to the Director of Electronic Service Delivery with respect to the adoption of procedures and standards specified under these rules; and
  - He has installed facilities and infrastructure needed for efficient delivery of electronic services and in an error-free manner in terms of norms laid down by the Director of Electronic Service Delivery and confirm the same in writing or through email duly signed by digital signature to the Director of Electronic Service Delivery.

- ***Authorised Service Provider to collect service charge*** - (1) The application for an eservice submitted by a user to an authorised Service Provider or an authorised agent shall be accompanied by such service charge as may be determined by the Director of Electronic Service Delivery which is payable in cash to the authorised Service Provider, at the time of making the application.[115]

---

[113]Alanezi, M A, Kamil, A and Basri, S (2010), "A proposed instrument dimensions for measuring e-government service quality", International Journal of u- and e-Service, Science and Technology, Vol 3 No 4, pp 1-17

[114] Bhattacharya, Debjani& Gupta, MP (2012) E-service quality model for Indian government portals: Citizens' perspective. Journal of Enterprise Information Management

[115] Carter, L. and Be´langer, F (2005), "The utilization of e-government services: citizen trust, innovation and acceptance factors", Information Systems Journal, Vol 15, pp 5-25

- The Director of Electronic Service Delivery may determine service charges by notification for e-services.
- The service charges may be different for different e-services such as, -
    - The status enquiry;
    - print-outs related to e-services;
    - The scanning of documents related to e-services;
    - The acknowledgement receipt; and
    - Any other e-service.
- The service charge shall not include any duly authorized taxes, charges, dues or any other moneys due in respect of service payable by any person to the Competent Authority concerned that are otherwise payable under the respective Act, Rule, Regulation or order of the Government when making an application to the concerned Competent Authority.
- ***The fee to be collected by the service provider-***
    a. Any fee or duly authorized taxes, charges, dues or any other money due in respect of a service payable by any person to the Competent Authority concerned that are otherwise payable under the respective act rule, regulation or order of the government when making an application to the concerned Competent Authority, shall also be collected by the authorised Service Provider or the authorized agent as the case may be, except for those payments that are ordinarily required to be made in the form of court fee stamps or treasury challans.

    b. The fee collected by the authorised Service Provider or the authorised agent shall be remitted with the Government treasury as may be determined by the Director of Electronic Service Delivery by the authorised Service Provider or the authorised agent as the case may be, in its entirety.
- ***Remittance or service charge and fee by the service provider-***
  Out of the service charge collected by the authorised Service Provider or the authorised agent for an e-service, a percentage of the service charge as may be determined from time to time by the Director of Electronics Delivery may be apportioned to the Government.

- The share of the Government out of the service charge so collected shall be remitted by the Authorised Service Provider or the authorised agent to Government treasury as may be determined by the Director of Electronic Service Delivery.[116]
- ***Presumption with regard to service charge paid to service provide and other conditions of obtaining e-services***- (1) Where any person pays a service charge to an authorised Service Provider or an authorised agent in respect of any notified e-service, the print-out or the electronic prompt acknowledging the payment in the relevant form and manner as may be determined by the Director of Electronic Service Delivery and provided to such person by the authorised Service Provider or authorised agent shall normally be taken as proof of such payment and it shall be presumed that in normal circumstances the dues or claims, for which the acknowledgement is purportedly issued, have been satisfied to that extent. (2) The payment of service charges to the authorised Service Provider or the authorised agent shall by no means create any right or title, temporary or permanent in nature in favour of a person concerned regarding obtaining the notified e-services. (3) Mere payment does not necessarily ensure the delivery of services if all conditions associated with the delivery of the service are not met fully at the time of making payment to the authorised Service Provider or the authorised agent.[117]
- ***Receipt or payment of money by or in favour of Government adopting the system of Electronic Service Delivery***-

  The receipt or payment of money by or in favour of Government adopting the system of Electronic Service Delivery shall be deemed to be a receipt or payment effected in compliance with the Financial Code and Treasury Code of the Government.[118]
- ***Filing of form, application or any other document***-

  Any form, application or any other document referred to in clause (a) of sub-section (1) of section 6 of the Act may be filed with any office, authority, body, agency or authorised Service Provider authorised by the Government of National Capital Territory of Delhi using the application software specified by it.

[116]Chawla Rajeev and MukerjiAnirban (2007), E-Governeance Initiatives of Karnataka", Yojana, Vol 51, pp 26-29
[117]Heeks, Richard (1999), "I-Development, not E-Development", Journal of International Development, Vol 14(1), pp1-11
[118] Holmes, D (2001), E-Gov: E-Business Strategies for Government, Nicholas Brealey, London

(2) The office, authority, agency or authorised Service Provider referred to in sub-clause (1) shall, while developing such software, take into account the following features of the electronic record, namely:- (a) lifetime; (b) preservability; (c) accessibility; (d) readability; (e) comprehensibility in respect of linked information; (f) evidentiary value in terms of authenticity and integrity; (g) controlled destructibility; and (h) augment ability.

Issue or grant of any license, permit, sanction or approval-

- Any license, permit, sanction or approval referred to in clause (b) of sub-section (1) of section 6 of the Act may be issued or granted by using the application software specified under rule 15.
- The license, permit, certificate, sanction or approval so issued shall be in the form prescribed in the respective Act, rule, regulation or order and shall contain the name and designation of the signing authority who had digitally signed and approved the electronic record along with the date and time of the creation of such record.
- ***Creation or repository of digitally signed electronic records***- (1) The Competent Authority may, as soon as, after the coming into effect of these rules create, establish and maintain a repository and database of digitally signed electronic records together with the associated application software and workflow to enable authorised Service Provider or the authorised agents to access such licenses, permits, certificates, sanctions or approvals, as the case may be, and deliver them to the user.[119]
- The relevant security procedures, as specified by the Government, shall be followed by such Competent Authorities, in respect of the electronic data, information, applications, repository of digitally signed electronic records and information technology assets under their respective control.
- ***Procedure for making changes in a repository of digitally signed electronic records*** -
    a) Any Competent Authority or any signing authority, either suomotu, or on an application by an interested party, may make or order to make an appropriate change in a repository of digitally signed electronic records, after following the procedure prescribed in the respective Act, rule, regulation or order.

[119]Kochhar Sameer and Dhanjal (2005), "E-Governance Report Card", Yojana, Vol 49, pp 60-69

b) Any such authority shall have privileges for making or ordering changes only in respect of the electronic records pertaining to its own jurisdiction.

1.6 LET'S SUM UP

In this chapter, we have studied the meaning of electronic delivery and the duties of competent authority to notify the list of public services to be delivered through electronic mode. We also discussed the powers and functions of the director of electronic service delivery. Finally, we have ended the discussion with the electronic delivery of services bill introduced in the Parliament of India in 2011.

1.7 FURTHER READING

- Adb.org (2019), https://www.adb.org/sites/default/files/publication/467826/adbi-wp890.pdf (last visited Nov 19, 2019).
- Nazir, Mohsin&Wani, Sani&Arif, Tasleem. (2014). Current Scenario of the e-Governance Related Initiatives in India.
- Isec.ac.in (2019), http://www.isec.ac.in/WP%20-%20165.pdf (last visited Nov 19, 2019).
- https://www.nisg.org/files/documents/D01010001.pdf

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is the aim of Electronic Delivery of Services Bill (EDS), 2011?

A. The aim of Electronic Delivery of Services Bill (EDS), 2011 is aimed at bringing transparency in public dealings and checking corruption in public dealing. The EDS Bill allows for "delivery of public services through electronic mode including the receipt of forms and applications, issue or grant of license, permit, certificate, sanction or approval and the receipt and payment of money.

2. What are the main Functions and Powers of Director of Electronic Service Delivery?

A. To authorise, suspend or terminate the services of the Authorized Service Providers; To determine norms relating to the selection of authorised agents by the authorised Service Providers and authorised agents; To determine functions, responsibilities and liabilities of authorised Service Providers and authorised agents; To determine norms on the service levels to be complied with by the authorised Service Providers and authorised agents; To determine service charges to be charged by the authorised Service Providers and authorised agents for providing e-services; To determine terms and conditions relating to the authorisation, suspension or termination of the services of the authorised Service Providers and authorised agents; and To make a alternative arrangements for delivery of e-services, in case of such suspension or termination of services of authorised Service Providers and authorised agents.

3. What is the stipulated timeline for the competent authority to publish the list of all public services to be delivered through electronic mode?

A. 180 Days.

1.9 ACTIVITY

Elaborate the pros and cons of the Electronic Delivery of Services Bill, 2011 along with the critiques with respect to it. (800 words)

Unit 2: Rules and Regulations related to Cyber Cafe

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Cyber Crimes through Cyber Cafes
- Rules and Regulation governing Cyber Cafes
- Due Diligence pertaining to the establishment of Cyber Cafes

1.2 INTRODUCTION

Cyber Cafe is internet access point for public and it is been observed that public access point are the most obvious places used by cybercriminals, where visitor data can be usually hacked due to lack of awareness of Cyber-crime in Visitors as well as their identity is difficult to reveal as they are making use public internet point.[120] Many Cyber Cafes are now providing Wi-Fi services for their customers. Due to lack of awareness of cybersecurity many Cyber Cafe Visitors make mistakes such as making use of unencrypted devices or protocols, not logging out after work is

[120]Rangaswamy, Nimmi. (2009)The non/formal business of cyber cafés: A case/study from India. J Inf., Comm, Ethics in Society

completed, simple password, same password for multiple sites, Information left on the hard drive, not clearing browser history, storing of data on public hard disk, not checking for illegal or malicious software before using public machine which results in loss to the Visitors. In 2013 report by Symantec 56 percent access their social networking account using public Wi-Fi unsecured network, 29 percent access their bank account, 54 percent access personal mail, 29 percent do online shopping, 3 out of 10 do not log off after using public Wi-Fi network and 39 percent do not take any special steps to protect themselves when using public Wi-Fi. Cyber-crimes can take place when pubic internet access points such as Cyber Cafes are used if security mechanisms are not used. Types of Cyber-crimes that have taken place through Cyber Cafe are credit card fraud by making use of key logger software, online share trading fraud, Email account hacking, phishing, Cyber terrorism, Malicious code like worms, virus etc.[121] Section 43, 66, 67, 69 and 70 of the Information Technology Act read with the relevant provision of Indian Penal Code, cover myriad of cybercrimes, which can be committed through Cyber Cafes-

- Harassment via a fake public profile on social network site;
- Online Hate community;
- Credit Card Fraud;
- Introduction of viruses, Backdoors, Trojans and Bugs;
- Cyber Terrorism;
- Online Sale of illegal Article;
- Cyber Pornography;
- Phishing and Email Scams;
- Tax Evasion and Money Laundering;
- Theft of Confidential information;
- Online Share Trading Fraud.
- Cyber Stalking

Information Technology Act 2000 is a legal framework created and implemented to prevent Cyber-crime and amendments have also taken place for it but still improvements are required.

[121]Haseloff, M A [2005], *Cybercafés and their Potential as Community Development Tools in India,* The Journal ofCommunity Informatics, Vol 1 no 3 pp53-64

Today Indian cyberspace has an increase in spam and phishing activities, spread of botnets, virus, worms and malicious code are also on the rise. This has made India to be figured out as an active source in spreading malicious infection in computers, which is generally observed in developing countries.

Cyber Crime is not defined officially in the IT Act or in any other legislation. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislation. Hence, the concept of cybercrime is just a ***"combination of crime and computer".***

1.3 LEGISLATIVE FRAMEWORK FOR CYBER CAFES IN INDIA

An Internet cafe or Cyber Cafe is a place, which provides Internet access to the public, usually for a fee. It includes any commercial establishment or Internet kiosk, the objective of which is to make Internet services available to the general public.The fee for using a computer is usually charged as a time-based rate. Cyber Cafe is considered to be a ***"Place of Public Amusement"***as defined under ***section 2 (9) of the Bombay Police Act, 1951 (Act XXII of 1951).*** In 1998 India introduced new Internet policy and Sify was the first ISP. Internet cafes are the primary form of Internet access for people as a shared access model, which is more affordable than personal ownership of computer system and Internet connections. LAN gaming centre was also one of the Cyber Cafe model where various players play game online. These players can be connected to various other players in some different locations.[122] These Cyber Cafes provide multiplayer games, which are popular. Gaming Cyber Cafe has a large demand in various countries by youth and children's and thus have become a popular model for earning the profit. Cybercafes have been started with the intention to provide Internet services and other services to its users. It is a definite place, where you can access the Internet for your emails, talking to your relatives through chat, voice and video. Cyber Café has become one of the businesses nowadays where you are charged in exchange for the services. The aforesaid café has several computer stations connected to LAN. There are resorts, hotels, motels and ships, which provides Internet access to the guests. Cyber cafés also give training to the person who does not know the usage of the

[122]Mancebo, François. (2003) Cybercafe

Internet and other activities available there. Cyber Café is defined under the Information Technology Act 2000 and rules and regulations to govern the cafes are mentioned under Information Technology Rules 2011.

1.4 GUIDELINES PERTAINING TO ESTABLISHMENT OF CYBER CAFES IN INDIA

In order to regulate Cyber Cafes, several states of India government Ministry of communication and Information Technology have passed regulations some under Information Technology Act (ITA) 2000 and some under the State Police Act. Now, the Information Technology Amendment Act, 2008 has made many significant changes in the prevailing laws of cyberspace applicable in India, one of which is regarding Cyber Cafes. Information Technology (Amendment)Act, 2008 has provided a specific definition for the term ***"cyber café"*** and also included them under the term ***"Intermediaries"***. Several aspects of the Act, therefore become applicable to Cyber Cafes. The government of India has taken initiatives by the mean of Act to provide cyber security for Cyber Cafe.[123]These are the following steps need to be followed by Cyber Cafes under ***Information Technology (Guidelines for Cyber Cafe) Rules, 2011***-

1. ***Registration of Cyber Café***

Under Rule 3 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 all cyber cafes shall be registered with a URN (Unique Registration Number) through an agency called as registration agency has been notified by the State Government in this regard. The requirements of registration shall include: Name of establishment, date of incorporation, Address with contact details including email address, Whether individual or partnership or sole proprietorship or society or company, Owner's name, Type of service to be provided from cyber café, Whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies).

2.*Identification Of User*

[123]'Cyber Cafes Under ITA 2008' (Naavi.org, 2020) <https://naavi.org/cl_editorial_09/edit_jan07_itaa_analysis_7_cyber_cafe.htm>

Under Rule 3 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 all Cyber Cafes should not allow any person to access the services of cyber café without user identity. The user is supposed to produce certain documents before having access to the services of the cyber café so that proper identification of the user is known. Such documents are as follows: Identity card issued by any School or College, Voter Identity Card or Permanent Account Number issued by Income-Tax Authority or Photo Identity Card issued by the employer or any government agency or Passport or Driving License issued by the Appropriate Government or Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

3.*Log Register*

In accordance with Under Rule 5 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011, after the identification of the user and any person associated with him has been established as per sub-rule (1) of rule 4, the Cyber Cafe shall register and maintain the required information of each user as well as associated person in the log register for a minimum period of one year.The Cyber Cafe shall maintain an online version of the log register. This online version of log register shall be checked by using digital signature and should contain details including Name, Address, Gender, Contact Number, Date, Type and detail of identification document, Computer terminal identification, Log in Time and Log out Time.

A monthly report of log register including date-wise details and use of computer resource shall be prepared and there shall be the submission of hard copy and soft copy to the agency of registration or person as pointed out by the registration agency by the 5th of every month.History of websites accessed by the user using computer resource at cyber café. Logs of proxy server installed at a cyber cafe. Cyber Cafe may refer to "Guidelines for auditing and logging – CISG-2008-01" prepared and updated from time to time by Indian Computer Emergency Response Team. Cybercafe shall ensure that log register is not changed and it is been maintained in a secure manner for a period of at least one year.[124]

4.*Management and Administration Of Physical Layout And Computer Resource*

[124]Keniston, K and D. Kumar, (2004) Ed *Bridging the Digital Divide: Experience in India*,London,Sage Publications

In accordance with Under ***Rule 6 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011,*** Cyber Cafes shall adhere to following guidelines-

1. Partitions of Cubicles put inside the Cyber Cafe, should not surpass four and a half feet in the range from the floor level.
2. The screen of all PCs introduced other than in Partitions or Cubicles should be confronted 'outward', i.e. they should confront the regular open space of the Cyber Cafe.
3. Any Cyber Cafe having work areas or segments might not enable minors to utilize any PC asset in desk areas or allotments aside from when they are recognized by their gatekeepers or guardians.
4. All-time checks and servers introduced in the Cyber Café of the PC framework should be coordinated with the IST (Indian Standard Time).
5. All the PCs in the cyber cafe might be furnished with the monetarily accessible security or separating programming in order to maintain a strategic distance from quite far, access to the sites identifying with erotica including kid smut or disgusting data.
6. Cyber Cafe should take vital measures to guarantee that their PC asset is not used for any unlawful activity.
7. Cyber Cafe might show on the PC that review the explicit destinations on PC is prohibited and one ought to do nothing which is against the law or illicit.
8. Cyber Cafe should make essential measures to not permit the client from meddling with the PC framework settings.
9. Client personality data and log enlist ought to be kept up by cyber bistro in a secure way.
10. Record of the cyber bistro's staff might be kept up for 1 year legitimately.
11. Cybercafe might not abuse or change the data in the log register Information Technology Rules-2011

5.*Investigation of Cyber Cafe*

In accordance with Under Rule 7 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 an officer authorized by the registration agency, is authorized to check or inspect cyber cafe and the computer resource of the network established therein, at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

A Cyber Cafe Owner is expected to preserve and retain such information as may be specified for particular duration and in such manner and format as the Central Government may prescribe and on failure to do so he may be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine. Thus, the responsibility of Cyber Cafes has now been clearly
defined with three-year imprisonment, which is also cognizable, bailable and compoundable.
There are many government stakeholder agencies formed for a secure computing environment and adequate trust and confidence in an electronic transaction.[125]

In India, many individuals go to Internet bistro to complete their everyday online exercises. Web cafes, or cybercafés, are spots that give administrations of web and different exercises and consequently clients need to pay them according to the time they have gotten to the administrations. Web cafes can be set up in genuine eating/drinking foundations, voyage ships, or different sorts of areas. Other than utilizing the PC workstation, you may likewise have the capacity to print or sweep reports, contingent upon the Internet cafe.[126] Yet, today the matter of Cyber Café has been declining in light of the fact that individuals get access to web at home, as they have the wideband association at home. Building up the cyber bistro is not a major ordeal, it has fewer prerequisites as contrast with different organizations however proprietors must be more secure on the grounds that cyber wrongdoing is been expanding in the present-day world.

1.5 LET'S SUM UP

[125]HaseloffAnikar M. - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 <http://ci-journal.net/index.php/ciej/article/view/226/181>
[126]GadgeReena K, Dr.MeshramB.B.,"Detect and Prevent Threats in Websites"-IJCST-International Journal of computer science and Techno- vol 3, Issue 1, Jan. - March 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

In this chapter, we have studied the meaning of cyber café along with a legislative framework for cyber cafes in India. Finally, we have ended our discussion with the guidelines that need to be followed by the cyber cafes as per the Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

1.6 FURTHER READING

- Singh, Umrav. (2016). Cyber Laws in India.
- Rangaswamy, Nimmi. (2009). The non/formal business of cyber cafés: A case/study from India. J. Inf., Comm, Ethics in Society. 7. 136-145. 10.1108/14779960910955855.
- Internet Privacy in India — The Centre for Internet and Society, Cis-india.org (2019), https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india (last visited Nov 20, 2019).
- Citeseerx.ist.psu.edu (2019),

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Cyber café?

Cyber Cafe isan internet access point for public and it is been observed that public access point are the most obvious places used by cybercriminals, where visitor data can be usually hacked due to lack of awareness of Cyber-crime in Visitors as well as their identity is difficult to reveal as they are making use public internet point.

2. Short note on legislative framework of cyber café in India?

An Internet cafe or Cyber Cafe is a place, which provides Internet access to the public, usually for a fee. It includes any commercial establishment or Internet kiosk, the objective of which is to make Internet services available to the general public.The fee for using a computer is usually charged as a time-based rate. Cyber Cafe is considered to be a ***"Place of Public Amusement" as defined under section 2 (9) of the Bombay Police Act, 1951*** (Act XXII of 1951). In 1998 India introduced new Internet policy and Sify was the first ISP. Internet cafes are the primary form of

Internet access for people as a shared access model, which is more affordable than personal ownership of computer system and Internet connections.

3. How do you register a cyber café?

Under Rule 3 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 all cyber cafes shall be registered with a URN (Unique Registration Number) through an agency called as registration agency has been notified by the state Government in this regard. The requirements of registration shall include: Name of establishment, date of incorporation, Address with contact details including email address, Whether individual or partnership or sole proprietorship or society or company, Owner's name, Type of service to be provided from cyber café, Whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies).

4. Short note on investigation of cyber café?

In accordance with Under Rule 7 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 an officer authorized by the registration agency, is authorized to check or inspect cyber cafe and the computer resource of network established therein, at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

A Cyber Cafe Owner is expected to preserve and retain such information as may be specified for particular duration and in such manner and format as the Central government may prescribe and on failure to do so he may be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine. Thus, the responsibility of Cyber Cafes has now been clearly

defined with a three-year imprisonment, which is also cognizable, bail able and compoundable.

1.8 ACTIVITY

Explain the guidelines pertaining to establishment of cyber café in India along with a case study. (1000 words)

Unit 3: Rules and Regulations related to Service Provider's Liability

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of Internet Service Provider
- Intermediaries Liability
- Liability of Service Provider and Section 79 of Information Technology Act
- Copyright Act and Intermediaries

1.2 INTRODUCTION

Origin of internet has raised many atypical issues that do not find an express solution in the existing legal dominion. The atypical power of scattering engendered by the web, a power that ordinary users can utilize, has created a new and grinding challenge to the ability of copyright

holders to enforce their ownership of intellectual property. The chief threat to copyright holders by the internet's untangle information distribution is online piracy. The scope of this problem is hard to define in concrete terms. Though the damage of online piracy is hard to evaluate in monetary terms, a driving motivation to protect the copyright holder remains. The widespread and open copyright abuse is feared and will a systematic cultural disregard for the author's intellectual property rights.

1.3 INTERNET SERVICE PROVIDER (ISP)

One of the salient features and equivocal issue associated with the fast-developing online industry is the liability of services providers are gateway to the world of cyberspace. They provide online access to individuals, educational, institutions, and government agencies. Those entities include online service providers, those who provide content through networks in addition to internet access, which is provided through the same networks and internet service providers who provide direct access to the internet and usually have content provided in direct location. The service providers are commercial and non- commercial entities that connect users to the internet, provided the user has access to the necessary hardware for this interface, namely telephone line and, modern and a personal computer.[127]

The liability of the service provider for copyright infringement can be fixed only when his position, powers and limitations are clearly understood. The Internet began as a closed network between government research laboratories and universities and colleges. As universities and colleges began giving Internet access to their faculty and other employees, ISPs were created to provide Internet access to those employees at home and elsewhere. The first ISP began in 1990 as The World, based in Brookline, Massachusetts.

Individual customers and businesses pay ISPs for Internet Access. ISPs are interconnected to one another at network access points. In turn, ISPs pay other, larger ISPs for their Internet access, which in turn pay still other ISPs. This cascades multiple times until transmissions reach a Tier 1 carrier, which is an ISP capable of reaching every other network on the Internet without

[127] B. Rowe, D Wood, D Reeves, and F Braun, "The Role of Internet Service Providers in Cyber Security", Institute for Homeland Security Solutions, Applied research* Focus result, 2011 <http://sites.duke.edu/ihss/files/2011/12/ISPProvided_Security-Research-Brief_Rowe.pdf>

purchasing IP transit or paying settlements. However, it is difficult to determine the status of a network because the business agreements to pay settlements are not made public.

1.4 LIABILITY OF NETWORK SERVICE PROVIDERS

According to section 79, of the IT Act[128]For the removal of doubts, it is hereby declared that "no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention."

Explanation.—for the purposes of this section,—

(a) ***"network service provider"*** means an intermediary; (b) ***"third party information"*** means any information dealt with by a network service provider in his capacity as an intermediary;

(b) This section seeks to restrict the liabilities of a network service provider in certain cases. Meaning of the term "network service provider" (NSP): Section 79 says that an NSP is an intermediary.

The IT Act has defined the term "intermediary" -

According to ***Section 2(1)(w) of the IT Act "intermediary"*** with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

1. It receives the message on behalf of another person, or

2. It stores the message on behalf of another person, or

3. It transmits the message on behalf of another person, or

4. It provides any service with respect to that message

[128](Cc.iitd.ernet.in, 2020)
<http://www.cc.iitd.ernet.in/misc/liability-network-service-providers.pdf> accessed 24 April 2020.

The term ***"electronic message"*** has not been defined in the IT Act. The UNCITRAL Model Law on E-commerce defines a data message as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy".[129]

Note: The IT Act has been based largely on the UNCITRAL Model Law on Ecommerce.

The IT Act has inserted ***section 88A into the Indian Evidence Act.*** This section relates to an electronic message forwarded through an electronic mail server. After considering the definition of data message under the UNCITRAL Model Law and the context of electronic message under section 88A of the Indian Evidence Act, it may be concluded that the term NSP is a narrow term that relates to electronic message service providers only (such as email service providers). It does not apply to other service providers such as search engines, auction websites etc. Even for Internet Service Providers (ISP), the benefits of this section would extend only to the email, voicemail, telephony etc services provided by them and not to the Internet connection services offered by them. However, this section must be read in conjunction with ***section 85 of the IT Act*** that relates to liabilities of companies. This is discussed in the next chapter of this book.

The restrictions on the liabilities of NSPs. An NSP is not liable for any third party information or data made available by him if:

1. The NSP proves that the offence or contravention was committed without his knowledge, or
2. The NSP proves that he had exercised all due diligence to prevent the commission of such offence or contravention.

The important terms used in this section are: Knowledge implies "clear perception of a fact" or ***"specific information".*** Liability of ISPs in India In respect to ISPs in India, their liabilities are also determined by the License for Internet Services based on guidelines dated 24th August, 2007. The license as applicable on 30th October 2007 is provided in the CD ROM accompanying the ASCL publication titled ***"Fundamentals of Cyber Law".***

<u>According to clause 33 of this license:</u>

[129] H E Pearson, "Liability of Internet Service Providers", 1996 <http://www.leginetcy.com/articles/Liability%2 0of%20Internet%20Service%20Providers.pdf>

1. ISPs must prevent unlawful content, messages or communications from being carried on their network. This includes objectionable, obscene, unauthorized and other content.[130]

2. Once specific instances of such content are reported to the ISP by the enforcement agencies, they must immediately prevent the carriage of such material on their network.

3. ISPs must ensure that content carried by them does not infringe "international and domestic cyber laws".

4. The use of ISP networks for anti-national activities would be construed as an offence punishable under the Indian Penal Code or other laws.

5. ISPs are required to comply with the IT Act provisions. They are responsible for any damages arising out of default in this compliance.

6. ISPs must ensure that their networks cannot be used to endanger or make vulnerable a networked infrastructure.

7. ISPs must ensure that their services are not used to break-in or attempt to break-in to Indian networks.

8. ISPs must provide, without any delay, all the tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through their equipment and network. These tracing facilities are to be provided to authorized officers of Government of India including Police, Customs, Excise, Intelligence Department officers etc.

9. ISPs must provide necessary facilities to the Government to counteract espionage, subversive acts, sabotage or any other unlawful activity.

1.5 INTERNET SERVICE PROVIDERS LIABILITY IN INDIA

In India, the law applicable to the infringer swing upon which part of law deals with that certain infringement. Therefore, due to the lack of such law, the Copyright Act and the Information Technology Act includes the liability of ISP's:[131]

[130] What is an Internet Service Provider (ISP)? - Definition <https://www.techopedia.com/definition/2510/internet-service-provider-isp>

- ***Copyright act 1957***

As per ***Section 51(a) (ii) of the Copyright Act***;

"the Indian Copyright Act, the act of infringement is when, a person without any license by the registrar or the owner of the particular copyright, does an act that is in the contravention of the conditions of a that license or condition imposed by a competent authority under this Act permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he is unaware as and had no reason to believe that the particular communication to the general public would result in copyright infringement."

Nowadays the Internet service providers, instruct their servers transmit and store their users' data across the network. This act of ISP's helps them to hold any third party liable in case of any infringement. In order to be liable for the infringement, it is very necessary that the ISP should benefit financially from it. The ISP's earn even if they offer some copyrighted illegal material because of the advertisements that come along with it. Therefore, an ISP can be held liable not only when they transmit such infringed material but they are liable even if they store it.

- ***Criminal Liability***

An ISP can be held criminally liable when he does an act of infringement or abets infringement of:

(a) the copyright in a work, or

(b) any other right conferred by this Act, If a person does such an act than the Copyrights Act provides for the punishment to be given to him, i.e of imprisonment which may extend to one year, or with fine, or with both.[1]

However, the Copyright Act clearly states that the ISP can be held liable only in the case he was unaware infringing material stored or being transmitted through their servers. This provides an exception to the liability.

- Information Technology Act, 2000

---

[131]Liability of Network Service Providers
<http://www.cc.iitd.ernet.in/misc/liability-network-service-providers.pdf>

Section 79 of the Information Technology Act states the ISP (a Network service provider in the case of this act) as an "Intermediary", which is defined as " any person who on behalf of any other person receives, transmits or stores any message or provides any service with respect to any message."[2] This section also provides that, no ISP can be held liable if he proves that he was unaware of the infringement that was caused by the third party that he had exercised all due diligence to prevent the commission of such offence.[132]

Therefore, the ISP can get away from being liable for the copyright infringement if it is proved under this section[3]

(a) That the ISP was unaware of the infringement,

(b) That he took all the due diligence to prevent such infringement.

However, data has passed through an ISP's servers or stored in them, that is likely to infringe the copyright of another, it is considered that such ISP had to have 'knowledge' of such data and he has the duty to take appropriate measures to prevent such infringement. In such a case, the ISP cannot take a defence that he was unaware of such infringement.

A person is said to have done an act with due diligence when in the layman's terms he had done that act or prevented an act by reasonable standards expected out of a prudent person who is said to have the knowledge about such illegal activity.[4]

- Drawbacks of Copyright Act

(a) The IT Act provides wider scope to the authorities to harass ISPs in matters where their liability is the question.

(b) Which actions can be termed as done with 'due diligence' is not defined anywhere in the act.

(c) Who is an ISP? The answer to this question is not given under the IT Act. Also, the IT Act does not provide for the liability of the ISP. The liability of ISP is as same as for anyone who is simply a communication carrier.

[132]Network Service Providers Not to be Liable
<https://meity.gov.in/content/network-service-providers-not-be-liable-certain-cases>

There is an urgent need to incorporate certain laws or bring amendments in the acts because the absence of specific laws regarding the liability of the ISP in the Indian Law results in the ISP's escaping the liability in case of infringement. In order to make way for resonate legislation with regard to ISP liability in India, it is essential to label some of the key subjects mentioned hereunder;

a) There is an acute need to provide a definition of Internet Service Provider. Unless it is done, it would always create confusion as to who can be put under the liability. It is also important to define "due diligence"

b) Effective tools like DCMA can be used. Various effective measures should be adopted so that the liabilities of ISP's are clearly identified.[133]

c) It should be made sure that, the Information Technology Act makes it obligatory for ISPs to terminate services of subscribers who frequently violate.

1.6 LET'S SUM UP

In this chapter, we have studied the concept of Internet Service Provider along with the liability of network service provider and provisions pertaining to it. Finally, we have ended our discussion with Internet Service Provider's liability in India and the relation between intermediaries and Copyright Act.

1.7 FURTHER READING

- Suresh.T.Vishwanathan.,*"The Indian Cyber Law"*, 1st Edition, 2000, Bharat Law House, New Delhi, p.96.
- Prof.S.R. Bhansali., *"Information Technology Act, 2000"*, 1st Edition, 2003, University Book House Pvt. Ltd, Jaipur, p. 218.
- NandanKamath., *"Law Relating to Computers, Internet and E-Commerce"*, 2nd Edition, 2000, Universal Law Publishing Co.Pvt.Ltd, Delhi, p. 2.

[133]Copyright Infringement And The Liability Of Internet <https://blog.ipleaders.in/copyright-infringement-liability-internet-service-providers/>

- Rahul Matthan., *"The Law Relating to Computers and the Internet"*, 2000, Butterworths India, Delhi, pp. 428-429.
- Raman Mittal., *"Online Copyright Infringement Liability of Internet Service Providers"*, 46 JILI (2004), p. 289.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Internet Service Provider?

They provide online access to individuals, educational, institutions, and government agencies. The service providers are commercial and non- commercial entities that connect users to the internet, provided the user has access to the necessary hardware for this interface, namely telephone line and, modern and a personal computer.

2. Define 'Intermediary' under IT Act?

According to section 2(1)(w) of the IT Act "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

3. What are the characteristics of NSP?

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

- It receives the message on behalf of another person, or
- It stores the message on behalf of another person, or
- It transmits the message on behalf of another person, or
- It provides any service with respect to that message.

4. What is the liability of the ISP under Copyright act?

As per Section 51(a) (ii) of the Copyright Act, "the Indian Copyright Act, the act of infringement is when, a person without any licence by the registrar or the owner of the particular copyright, does an act that is in the contravention of the conditions of a that licence or condition imposed by a competent authority under this Act permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement

of the copyright in the work, unless he is unaware as and had no reason to believe that the particular communication to the general public would result in copyright infringement."

1.9 ACTIVITY

Explain the liability of Internet service providers in India with an illustration or case study. (800-1000 words)

Unit 4: E-Health and Regulatory Framework

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept, functionalities and benefits of E-Health
- Electronic Health Records
- Enactments of different laws pertaining to E-Health

1.2 INTRODUCTION

As per the World Health Organization ("WHO"), E-Health means "the use of information and communication technologies ("ICT") for health". The definition, though very concise, is not very helpful. The European Commission has put forth a more elaborate definition of e-Health. e-Healthrefers to "tools and services using information and communication technologies that can

improve prevention, diagnosis, treatment, monitoring and management". Therefore, the expression e-Health may be safely said to include both tools and services that use ICTs for purposes connected to health.[134]

For several years now healthcare services have been facing pressure by citizens, patients, professionals and also by public and private institutions. The ageing of the population, higher standards of living, and more informed and educated citizens mean that both patients needs and patient expectations are growing. These rising demands, along with the appearance of new and costly health technologies and increasing budget restrictions, invite health managers to invest wisely in ICT and to carefully assess its opportunity cost in the current context of rising health expenditure and economic crisis.[135]

Investment in eHealth should be considered a decision of key importance for the health system. This means there must be, in addition to an accurate estimate of costs, an evaluation of its benefits, both in economic terms and in terms of improved quality and efficiency in the services provided. Nowadays, ICT tools must be included among the many instruments used in a health system, whose functioning can hardly be conceived without tools of this type.

1.3 CONCEPT, FUNCTIONALITIES AND BENEFITS

The concept of eHealth encompasses applications as diverse as electronic health records, different types of telemedicine, epidemiological surveillance, health portals, management systems and distance learning programs focused on health and medicine. Its users and beneficiaries are equally diverse. The applications help meet the needs of health professionals, those of patients and their families, those of healthcare authorities and experts and also those of input and service providers, among others.

There can be no doubt that eHealth represents an equitable, effective and efficient way to increase accessibility, safety and quality in healthcare. eHealth tools can be used to increase the availability of medical resources, thus optimizing care processes. They enable specialized

[134] Michael Kirby, Medical Technology and New Frontiers of Family Law, 1 AUSTL J FAM L 196, 212 [1987]
[135] Oh, Hans &Rizo, Carlos &Enkin, Murray &Jadad, Alejandro. (2005). What is eHealth? A systematic review of published definitions. World hospitals and health services: the official journal of the International Hospital Federation. 41. 32-40

knowledge to be taken to different places or to isolated locations, through distance appointments or teleconsultation. They facilitate the provision of timely healthcare, partnership projects, etc. They can also help reduce the costs incurred by systems and by families.[136]

In eHealth, two large spheres can be distinguished from one another, for purposes of analysis. There is, on the one hand, what is known as health informatics, that is, technological solutions for applications used to provide care, which allow information to be recorded and processed: electronic health records and department-specific applications, population management systems and systems that support planning and management are a few examples. And, on the other hand, there is telemedicine, which refers to health services and care provided from a distance. Applications already exist for many of the specialities: tele radiology, tele cardiology, tele dermatology, tele ophthalmology, tele pathology, tele psychiatry, and others.[137]

The case of tele radiology is a clear example of the advantages of telemedicine. Small or rural communities that cannot sustain an on-staff radiologist can benefit a great deal from the professional activity performed at a distance. Local hospitals can send images to a larger care center in order to obtain a second opinion, whether from the general radiologists who work in such centers or from radiologists with particular subspecialties. Emergency rooms can send, any time day or night, their images to affiliated centers or even to the homes of radiologists. Tele radiology as a teaching tool, can also enhance the quality of ongoing medical training. And finally, tele radiology offers direct benefits to the patient, by reducing the costs of transportation, accommodations and board that would be incurred if the patient had to travel to where the doctor is based.

The use of ICT can also bring significant improvements to the management of public health, in terms of areas of surveillance and also in the planning and overseeing health service management. ICT tools contribute to the design of safer, timelier and more reliable processes for data gathering and storage and also to better statistical use of the information. This has positive repercussions on the effectiveness and efficiency of the macro system that encompasses

[136] Ashok VikhePatil, K V Somasundaram and R C Goyal; Current Health Scenario In Rural India <http:// www.sas.upenn.edu/~dludden/WaterborneDisease3.pdf>

[137] Awski, Szymon&Saberwal, Gayatri. (2014). IneHealth in India today, the nature of work, the challenges and the finances: An interview-based study. BMC medical informatics and decision making. 14. 1. 10.1186/1472-6947-14-1

everything from the analysis of health needs and problems to the evaluation of health outcomes obtained in the population.[138]

1.4 ELECTRONIC HEALTH RECORDS

An Electronic Health Record (EHR) is a digital version of a patient's health records. EHRs help eliminate the problems associated with physical records such as loss and lack of accessibility. EHRs can be stored centrally and accessed at any time, irrespective of where or when the information was collected. With EHRs, doctors are able to view their patient's complete medical history even if they are treating the patient for the first time. This would help reduce duplication of tests and facilitate the secure exchange of information, which in turn helps the patient and the healthcare facilities manage costs.

1.5 BASIC FUNCTIONS AND ELEMENTS OF EHR

While EHRs were initially developed to document clinical care, most can perform additional functions that can support good quality care. Common functions of EHRs include (Health Resources and Services Administration, 2014a).

- Recording patient demographics and care management data on patient visits.
- The clinical decision supports.
- Reports required for financial management, quality assurance, chronic disease management, and public health data collection.
- Consents, authorisations, and directives.
- Interfaces and interoperability required to exchange health information with other clinicians, laboratories, pharmacies, patients, and government disease registries.
- e-prescribing.
- Alerts and reminders.
- Medication reconciliation.

[138] Marcus E, Fabius R. What is E-health?
<http://www.acpenet.org/ Forums/Topical/Ehealth/Primer.htm>

- Commonly used screening tools and checklists.
- commonly used forms for schools, camps, and sports participation.
- Patient education.

Some systems might also include integrated practice management support that enables functions like billing, online scheduling, and patient portals. Examples of some basic elements of EHRs are provided below. This list is not exhaustive and designed to provide a glimpse into EHRs and some of their capabilities.

Some of the benefits of EHR can be classified into the following types:

- ***Accessibility and Availability***

Paper charts are for single users; they can only be seen by one person in one place. EHRs can be used by more than one person at a time, and they can also be accessed from different locations. This is one of the benefits that new users most quickly come to appreciate.[139]

- ***Multiple display modes***

EHRs also have the potential of offering various ways to view the information, since users sometimes prefer to see information in different formats depending on their needs. A good EHR must allow data display to be configured in different ways, offering these options to users. Another useful function in clinical practice is to be able to view trends. These can be generated instantly, by putting the trends shown by a lab value or a vital sign (such as blood pressure) into graphic form.

- ***Communication with other professionals***

EHR systems can serve as vehicles for communication among professionals. This capability need not be limited to physician-to-physician communication, but can also include other members of the healthcare team. Many EHR systems include features similar to e-mail or instant messaging, thus allowing the different professionals to send messages to other professionals involved in the care of this patient.

- ***Communication with patients***

[139] Bhatia JC, Cleland J: Health-care seeking and expenditure by young Indian mothers in the public and private sectors. Health Policy Plan 2001, 16(1):55–61

EHRs can also improve communication with patients. As mentioned above, the personal health record can potentially be used as a communication channel between the patient and the health team caring for the patient.[140]

- ***Data aggregation***

EHR systems also have data collection capabilities, which makes it possible to create data groups and summaries. To ensure effective data aggregation, it is vital that data quality be very carefully controlled and that medical knowledge is correctly represented (through the use of semantic constraints). This functionality can be applied to the reuse of stored information for purposes of clinical management, clinical research or the preparation of public health reports.

- ***Access to knowledge bases***

Another potential benefit of using an EHR system is that it permits access to knowledge bases in a contextual manner. This means that the EHR can provide contextual information concerning each patient and provide the user with information that is useful in decision-making, extracted from different knowledge bases.

- ***Integration with decision-making support systems***

Decision-making support is the ***raison d'être*** of EHRs. The aim of these applications is to contribute to the care process, offering support to professionals, showing updated contextual information and suggesting alternatives to their decisions. These computerized decision-making support systems are difficult to achieve and are not very advanced due to the complexity inherent in their development and implementation. They consist of a rule engine that uses information based on the patient (from his or her EHR) and information based on scientific knowledge (from the system's knowledge bases), with which they generate different outputs, such as reminders, alerts, diagnostic or treatment suggestions based on the automation of clinical practice guides, etc. Their ultimate goal is to prevent errors and to enhance care quality.[141]

- ***Cost benefits***

The issue of whether EHR system implementation brings cost benefits is a controversial one, with literature containing evidence in both directions. This inconsistency arises in part because of

[140]Loman P. E-Health: 'Putting health on the Net'. An FCG White Paper <http://www.fcg.com/webfiles/whitepaper/white_paper_files/wpEhealth.asp>

[141] Reddy KS, Patel V, Jha P, Paul VK, Shiva Kumar AK, Dandona L: Towards achievement of universal health care in India by 2020: a call to action. Lancet 2011, 377(9767):760–768

the different perspectives used for analyzing returns on investment (ROI) (the individual physicians, service providers, insurance companies, governments) and the type of health care system that predominates in each country. More information is needed before more precise calculations can be made of the ROI related to EHR systems.

1.6 INVESTMENT IN E-HEALTH

The healthcare sector as an industry is expanding rapidly in India and has not been as severely impacted by the economic slowdown as some of the other industries.India, one of the biggest emerging markets, is currently an important destination for Foreign Direct Investment ("FDI").[142]A significantly low presence of doctors in rural and semi-urban areas has led to limited access to proper healthcare facilities for people living in these areas. Telemedicine and e-Health are considered to be some solutions to this lack of access. The growth of the IT sector in India (which plays a crucial role in telemedicine) has led to the emergence of this sector in India. Tele-radiology has emerged as a fast-growing area with an increasing number of foreign hospitals active in this space. These hospitals consult Indian experts to provide opinions, i.e., on x-rays of patients in the hospital. Many hospitals have adopted the public-private partnership route to render services through telemedicine.

Some investment options are:

a) FOREIGN DIRECT INVESTMENT

Foreign investment into India is governed by the Foreign Exchange Management Act, 1999 ("FEMA"), the rules and regulations made by the Reserve Bank of India ("RBI"), and the Industrial Policy and Procedures issued by the Ministry of Commerce and Industry through the Secretariat for Industrial Assistance, Department of Industrial Policy and Promotion ("DIPP").[143]

The provisions pertaining to FDI are laid down in Schedule I of FEMA (Transfer or Issue of Security by a Person Resident outside India) Regulations, 2000.While the DIPP issues policy

[142] Oracle Corporation. CEO Perspective: Health Care Information Technology <http://www.hciv.com/profiles/oracle.pdf>

[143] Consolidated FDI Policy, Government of India, Ministry of Commerce & Industry, Department of Industrial Policy & Promotion, SIA (FC Division) <http://dipp.nic.in/ English/policies/FDI_Circular_2016.pdf>

guidelines and press notes/releases from time to time regarding foreign investment into India, it also issues a consolidatedpolicy on an annual basis ("Consolidated FDI Policy"). Currently, foreign investment is regulated by the Consolidated FDI Policy of 2016.100% FDI is permitted in most sectors under the automatic route, i.e., where prior approval of the government, specifically the Foreign Investment Promotion Board ("FIPB"), is not required. Generally, there are no restrictions prescribed for e-Health services, and therefore FDI up to 100% should be permitted without government approval. It may also be noted that FDI is permitted up to 100% under the automatic route in the hospital sector and the manufacture of medical devices. In the pharmaceutical sector, FDI is permitted upto 100% in Greenfield projects and 74% in Brownfield projects under the automatic route and FDI beyond 74% in Brownfield projects requires FIPB approval. Greenfield projects are new projects that are coming up in India while Brownfield projects are existing projects in India.

b) FOREIGN VENTURE CAPITAL INVESTMENT

Another vital means of investment is through venture capital investment by entities registered with the Securities Exchange Board of India ("SEBI") as foreign venture capital investors. While it is not mandatory for a private equity investor to register as a Foreign Venture Capital Investor ("FVCI") under the FVCI regulations,[144] there are some significant advantages to be gained by registering as an FVCI. An FVCI is exempt from compliance with the pricing guidelines under the Consolidated FDI Policy for the acquisition of securities at the time of entry as well as for the transfer/sale of securities at the time of exit. Secondly, in cases where thepromoters of the company intend to buy back the securities from an FVCI, they are exempted from making an open offer under the Takeover Code. It should be noted that SEBI has been granting approvals to FVCIs only for investments in certain identified sectors, amongst them being researchand development of new chemical entities in the pharmaceutical sector, and units of SEBI registered Venture Capital Funds ("VCFs"). Further, the Reserve Bank of India ("RBI") has made recent amendments to the foreign exchange control regulations to permit FVCIs to invest in SEBI registered Alternate Investment Funds ("AIFs").[145]

[144] SEBI (Foreign Venture Capital Investor) Regulations, 2000

[145] SEBI introduced SEBI (Alternate Investment Funds) Regulations, 2012 to govern domestic pooling vehicles. RBI has issued Notification no. FEMA. 355/2015 that permits AIFs and other investment vehicles to accept foreign investments under the automatic route

1.7 LEGAL AND REGULATORY FRAMEWORK

a) THE I.T. ACT, 2000

E-Health involves a constant exchange of information between the patient and the service provider. The patient's personal information, such as medical history and physiological conditions, are considered Sensitive Personal Data or Information ("SPDI") under the Data Protection Rules.[146] When a body corporate collects, stores, transfers or processes such information, certain requirements under the Data Protection Rules are triggered.Consent is one of the major requirements under the Data Protection Rules. Before a doctor or an institution does anything with a patient's data, they are required by law to obtain the recipient's consent in writing. The patient must be informed about the fact that the data is being collected, what it will be used for and whether it would be transferred to any third parties, along with the contact details of the agency collecting the information.

The Data Protection Rules also mandate the implementation of reasonable security practices and procedures in order to keep the SPDI secure. This requirement is fulfilled if the body corporate conforms to the international standard IS/ISO/IEC 27001 on "Information Technology-Security Techniques-Information Security Management System-Requirements" or similar standards that are approved and notified by the Central Government. As on date, no such standards have been notified.

In 2013, the Ministry of Communications and Information Technology came out with a clarification[147]which stated that body corporates that were collecting, storing, processing or transferring information out of a contractual obligation were not required to observe some of the requirements of the Data Protection Rules such as obtaining consent from the owner of the SPDI for collecting or disclosing the SPDI. The other requirements, however, must still be observed.

[146] Rule 3 of the Data Protection Rules defines Sensitive personal data or information of a person to mean such personal information which consists of information relating to (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information

[147] Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000 issued on 18th March, 2013 <http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules_1.pdf>

b) OTHER SERVICE PROVIDERS REGULATIONS UNDER THE NEW TELECOM POLICY, 1999 (OSP REGULATIONS)

Service providers who render "Application Services" - which includes telemedicine services – using telecom resources provided by telecom service providers, are required to be registered as an 'Other Service Provider' ("OSP") with the Department of Telecommunications.

c) THE DRUGS AND COSMETIC ACT, 1940

The D&C Act and D&C Rules regulate the manufacture, sale, import and distribution of drugs in India. In many foreign jurisdictions, there is a clear distinction between a drug that must be sold under the supervision of a registered pharmacist on the production of a valid prescription (signed by a registered medical practitioner) and those that can be sold by general retailers over-the-counter ("OTC"). OTC drugs have a different meaning in the context of Indian laws. The D&C Act requires that all drugs must be sold under a license.

The D&C Rules also state that prescription drugs can only be dispensed on the production of a prescription which is in accordance with the provisions of the rules. For a prescription to be considered valid under the D&C Rules, it must be in writing, signed and dated by the doctor issuing the prescription.

d) THE INDIAN MEDICAL COUNCIL ACT, 1956

The MCI Act provides that only those persons who have a recognized degree in medicine and are registered with one of state medical councils have the right to practice medicine in India. The MCI Code lays down professional and ethical standards of interaction of doctors with patients. The MCI Code also specifies that efforts are to be made to computerize medical records so that they can be retrieved quickly. Doctors are bound by the MCI Code and are required to submit a declaration to that effect. The apex body currently regulating the practice of medicine is the Medical Council of India. However, the proposed National Medical Commission Bill, 2016,[148] which has been drafted by the National Institution for Transforming India ("NITI Aayog"), intends to replace the current Medical Council of India with a 'National Medical Commission'. The passing of the National Medical Commission Bill would see a change in the current regulatory framework regulating medical practitioners.

[148] Proposed National Medical Commission Bill, 2016
<http://niti.gov.in/writereaddata/files/document_publication/MCI%20Bill%20Final.pdf>

e) THE CLINICAL ESTABLISHMENTS ACT, 2010

Establishments falling under the definition of a 'clinical establishment' under the Clinical Establishments Act would be required to register with the relevant authority and conform to the minimum standards as prescribed under the act. The Clinical Establishments Act is applicable in Arunachal Pradesh, Uttar Pradesh, Uttarakhand, Rajasthan, Bihar, Jharkhand, Himachal Pradesh, Mizoram, Sikkim and all Union Territories except the NCT of Delhi. Certain states such as Maharashtra and Karnataka have their own state clinical establishment legislations.

1.8 LET'S SUM UP

The e-Health market presents a lot of opportunities, but with every opportunity, there are bound to be risks involved. Innovation in this sector is yet to reach a saturation point, with new products frequently being introduced in the market. The legislative framework to protect and regulate such developments will remain one step behind, as it is yet to be seen how the industry will mature. Regardless, regulators have taken note of the restrictions, and in many cases, the absence, of the law and are striving to formulate forward-looking policies and legislations. The NIPR is only one such example.

The Ministry of Health and Family Welfare recently set up ten panels led by the top brass of the DCGI'soffice. They have been entrusted with the revision of the drug regulations in order to bring about ease in compliance and adopting to the progressive changes in the industry.

1.9 FURTHER READING

- Gambarte, M. L., Lopez Osornio, A., Martinez, M., Reynoso, G., Luna, D., et al. (2007). A practical approach to advanced terminology services in health information systems. Stud Health Technol Inform, 129, 621-625.
- Greenes, R. A. (2007). Clinical decision support - the road ahead. Amsterdam: Elsevier Academic Press.

- Heimly, V., Grimsmo, A., Henningsen, T. P., &Faxvaag, A. (2010). Diffusion and use of Electronic Health Record systems in Norway. Stud Health Technol Inform, 160 (Pt 1), 381-385.
- McDonald, C. J. (1997). The barriers to electronic medical record systems and how to overcome them. J Am Med Inform Assoc, 4 (3), 213-221.
- Simon, S. R., Kaushal, R., Cleary, P. D., Jenter, C. A., Volk, L. A., et al. (2007). Physicians and electronic health records: a statewide survey. Arch Intern Med, 167 (5), 507-512.
- Sujansky, W. V. (1998). The benefits and challenges of an electronic medical record: much more than a "word-processed" patient chart. West J Med, 169 (3), 176-183.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is E-Health?

As per the World Health Organization ("WHO"), E-Health means "the use of information and communication technologies ("ICT") for health".

2) What is EHR?

An Electronic Health Record (EHR) is a digital version of a patient's health records.

3) What are the functions of EHR?

Common functions of EHRs include (Health Resources and Services Administration, 2014a).

- Recording patient demographic and care management data on patient visits.
- The clinical decision supports.
- Reports required for financial management, quality assurance, chronic disease management, and public health data collection.
- Consents, authorisations, and directives.
- Interfaces and interoperability required to exchange health information with other clinicians, laboratories, pharmacies, patients, and government disease registries.
- e-prescribing.
- Alerts and reminders.
- medication reconciliation.

- Commonly used screening tools and checklists.
- commonly used forms for schools, camps, and sports participation.
- Patient education.

4) How does the I.T. Act aid in E-Health?

The patient's personal information, such as medical history and physiological conditions, are considered Sensitive Personal Data or Information14 ("SPDI") under the Data Protection Rules. When a corporate body collects, stores, transfers or processes such information, certain requirements under the Data Protection Rules are triggered.

1.11 ACTIVITY

Explain the meaning, concept, functions and elements of E-Health and Electronic Health Records along with the legal enactments with respect it? (1000 words)

Block 4
Laws related to Data Protection in India

Unit 1: Law related to Sensitive Personal Data in India

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is Sensitive Personal Data or Information
- Procedure to collect the Sensitive Personal Information
- To whom can disclosure of information be made

1.2 INTRODUCTION

The Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) isn't exhaustive and did not specifically deal with the protection of electronic data, until the

Information Technology (Amendment) Act 2008 was passed and the IT Act, 2000 was amended accordingly to include certain provisions relating to electronic data. Further, to give effect to the then brought provision by the 2008 Amendment Act, the Central Government framed certain rules. Hence in the year 2011, the Central Government in exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the IT Act, 2000, passed the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information to deal with personal information and also defined sensitive personal information, with which we are concerned here.[149] These rules are called "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" (hereinafter referred to as the 2011 Rules).

1.3 LEGAL DEFINITION OF 'PERSONAL INFORMATION' AND 'SENSITIVE PERSONAL DATA OR INFORMATION'

The definition of ***"Personal information"*** is found under ***Rule 2(i),*** it has been defined as, any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. It is however different from Sensitive Personal Data or Information. Sensitive Personal Data or Information has been defined under ***Rule 3 of the 2011 Rules.*** It states that in respect of any person, the sensitive data or information is the one which consists of his information relating to:-

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;

[149] Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233

vii. any detail relating to the above clauses as provided to body corporate for providing service; and

viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

However, by virtue of the proviso to this rule, it excludes from its purview any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force.[150] And thus, this information which is so excluded by virtue of the proviso to Rule 3 isn't considered to be sensitive personal information for the purposes of the 2011 Rules.

1.4 PROCEDURE TO COLLECT THE SENSITIVE PERSONAL INFORMATION

The prerequisites of collecting or obtaining such data or information which has been covered under the definition of the Sensitive Personal Information as per ***Rule 3 of 2011*** Rules have been given under Rule 5 of the same. It includes:

(1) Consent

No Sensitive Personal Data or Information is permitted to be collected without the consent of the person whose information is being sought to be collected. Further, to ensure that this aspect of consent is well adhered to, the 2011 Rules provide that such consent by the provider must be in writing through letter or Fax or can be sent by email and the point worth noting is that the consent here is regarding the purpose of usage of such information. This consent is required before the collection of such Sensitive Personal Information or Data.

(2) Collection of Data must be necessary and for a lawful purpose

The 2011 Rules do permit the individual or entity to collect any information which would be covered under Rule 3 as Sensitive Personal Information or Data only when these 2 conditions are met:

(a) that the information which is sought to be collected is for a lawful purpose which is connected with any of his or its function or activity which in turn is also lawful; and

[150]Samuel Warren & Louis D Brandeis, "The Right to Privacy" Harvard Law Review 193 (1980)

(b) that collecting such sensitive personal data or information is necessary for that lawful purpose.

(3) Knowledge of the person giving the concerned information

The person or entity who is collecting information has to make sure:

(a)that the person whose information is being collected knows that such information is being collected;

(b) that the person whose information is being sought is aware of the purpose for which the concerned information has been collected;

(c) that such person is aware of the person/authority/institution who are likely to be the recipients of the information which is being sought from him;

(d) that such person knows certain details of the agency which is collecting such information as well as the one who will retain such information. Such information shall comprise of the names and addresses of the above-mentioned agencies.

And the person or entity seeking such sensitive personal information must take such reasonable steps as it deems fit and necessary to fulfil the conditions mentioned above.

(4) Also, the person or entity who is collecting the sensitive personal information is under an obligation to provide the person, from whose such information is sought, an option to not provide (or in other words, decline) whatever data or information which was sought to be collected. Discharge of this obligation has to be done by the concerned person or entity prior to collecting such data or information. It is worth noting here that this protection is available to all types of Personal Information, as covered by the 2011 Rules, and hence is also available to information or data other than that covered under sensitive personal data or information at par with the one which is so covered.[151]

(5) Withdrawal of Consent

Along with the prior mentioned right, the person from whom the information is sought also has the right to withdraw his consent which was earlier given. As a safeguard and to ensure that no

[151] Alan F Westin, "Science, Privacy and Freedom" 66 Columbia Law Review 1003 (1966)

one except the concerned person is withdrawing such consent, this withdrawal of consent id also required to be sent in writing.

(6) Information not to be retained for more than required time

Any person or entity who was retaining Sensitive Personal Data or Information is not permitted to retain such data or information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(7) Authorized Use of the Data or Information

As per the 2011 Rules, the information which is collected shall be used for only the purpose for which it has been collected and not otherwise.

(8) Permitting the Correction as well as Amended of the already provided information

Entity or the concerned person shall permit the persons by whom information was provided to review the information they had provided, as and when requested by them and shall ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.

(9) Keeping the Information secure in compliance with the 2011 Rules

Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

1.5 DISCLOSURE OF THE SENSITIVE PERSONAL INFORMATION OR DATA

The 2011 Rules under Rule 6 covers or encapsulates 3 methods whereby the disclosure of the Sensitive Personal Information is permitted, which will be discussed. As a caution, it is not to be confused with the "transfer of information' which is a different concept and will be addressed in the next heading. The 3 methods by which disclosure is permitted are :

(i) Disclosure to the third party by Prior Permission of the person who gave such information ;

(ii) Disclosure of Information to Government Agencies on certain grounds ;

(iii)Disclosure to the third party in compliance with an order passed under any law in force for the time being.

- ***By Prior Permission***

The Sensitive Personal Data or Information can be disclosed to any third party, provided that the person who has given such information has given his permission for such purpose. Such permission is not mandatorily required, for disclosing such information to the third party, if the information was shared under some sort of contract and that contract itself mentions that the parties agree to disclose such information. Another instance where such permission of the provider is not required is when the concerned person or the entity is under a legal obligation to do so.[152]

- ***Disclosure to Government Agencies***

Rule 6 of 2011 Rules provide certain situations wherein the Sensitive Personal Data or Information shall be shared with Government Agencies, even without asking for the permission of the provider of such information. The contingencies or situations under which the Government Agencies can obtain such data or information are:-

- for the purpose of verification of identity or
- for prevention, detection, investigation including cyber incidents or
- prosecution or
- Punishment of offences

Similar to this Rule 6 of 2011 Rules, Section 69 of the Information Technology Act, 2000, empowers the Central Government, State Government, and the persons specially authorized by Central or State Government in this behalf, to pass an order directing any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource, on any of the following grounds: -

- in the interest of the sovereignty or integrity of India ; or
- defense of India ; or

[152]Shrikant, Ardhapurkar&Srivastava, &Tanu, & Swati, Sharma &chaurasiya, Mr &Vaish, Abhishek. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. International Journal of Engineering Science and Technology 2

- security of the State ; or
- friendly relations with foreign States ; or
- public order ; or
- for preventing incitement to the commission of any cognizable offence relating to above ; or
- for investigation of any offence

- ***Disclosure to the third party under any law***

Rule 6 mentions that any Sensitive Personal Data or Information shall be disclosed to any third party by an order under the law for the time being in force.

1.6 TRANSFER OF INFORMATION

As mentioned above the disclosure of information is different from the transfer of information. In short, where disclosure is usually made to any person or entity which is independent from the one, the transfer is usually used when the information is exchanged between organizations or persons which are connected in a certain way.[153] Rule 7 of 2011 Rules, permits entity or authorized persons to transfer Sensitive Personal Data or Information, to any other body corporate or a person in India, or located in any other country, provided such intended recipient ensures the same level of data protection as provided for under the 2011 Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

1.7 FAILURE TO COMPLY WITH THE PROVISIONS

Since, 2011 Rules draw its powers from the IT Act 2000, there are certain provisions which provide for the contravention of certain provisions, and thus needs to be read for a better understanding of the concept at this point.[154]

[153] Privacy-Enhancing Technologies—approaches and development <http://www.sciencedirect.com/>
[154] Philip E. Agre, Marc RotenbergTechnology and privacy: the new landscape

Section 72A of the IT Act, 2000 provides punishment for disclosure of information, knowingly and intentionally, without the consent of the person to whom the information relates, and in breach of the lawful contract as imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

Further ***Section 43A of the IT Act,*** relates to Compensation for failure to protect data. This provision applies to those body corporate which possess, deal or handle any Sensitive Personal Data or Information in a computer resource which it owns, controls or operates, and is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person. The provision provides that in the situation mentioned above, such body corporate shall be liable to pay damages by way of compensation to the person who is so affected.

1.8 POINTS TO BE PONDERED UPON

In the definition of Sensitive Personal Information under Rule 3 of 2011 Rules, certain information hasn't found a place which by their very nature are sensitive and needs to be adequately protected, and at par with information which has already been given security. In the last few years, reliance on the internet has increased rapidly at an exorbitant rate, and people who use internet usually put certain information which are sensitive but aren't protected by any legal frameworks from being misused.[155] Further, more and more people are joining and regularly using social networking websites, and are readily using electronic communication to be in touch with others. Thus, it is time to give a serious thought about whether electronic communicationrecords including emails, chat logs and other communications made using a computer do not need to legally protected against any possible misuse.

1.9 RECENT LEGAL UPDATES

The Hon'ble Supreme Court of India by its judgment in the case of ***Justice K.S. Puttaswamy (Retd.) &Anr v Union of India &Ors (W.P. (Civil) No. 494 of 2012)***, recognized and

<http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61_nTcL_CnCl7Je2LcrQ&hl=en&ei=7L2YS_T2KYSysgOygbnCAQ&sa=X&oi=book_result&ct=result&resnu m=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false>

[155] Data Protection Act 1998: 1998 CHAPTER29
<http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1>

pronounced the right to privacy as a fundamental right which is given under the Constitution of India. This landmark judgment definitely calls for an update of the Indian Laws in respect of the Information Technology as well.[156] To achieve this, Personal Data Protection Bill, 2018 was drafted and it is likely to be placed in the upcoming session of the Parliament by the Ministry of Electronics and Information Technology. The Bill intends to regulate the processing of personal data of individuals by government and private entities which are incorporated in India as well as those which are incorporated abroad. The Personal Data Protection Bill 2018, needs to address a lot of things which yet have not been discussed from a legal viewpoint and have been overlooked by the laws which have been in force till now. In the recent updates also, there has been news of government asking certain messaging apps like ***'Whatsapp'*** to share the data with the government authorities. It seems fair from one point, but on the other hand if we look at it from an individual's point of view, the invasion and sharing of chat details of an individual with anyone against or without his consent seems to be in direct conflict with his right to privacy, which as mentioned has been accorded the status of Fundamental Rights. Thus, the least we may expect of the Personal Data Protection Bill, 2018 is to address the issues and conflicts which have already arisen. The Bill in whatever manner passed will have a very big impact on the Information Technology in the upcoming years, and thus should also be far-sighted.

1.10 LET'S SUM UP

In this chapter, we have studied what is Sensitive personal data or information and personal information along with its legal definition. Furthermore, we studied the procedure to collect sensitive personal information and to whom the information has to be disclosed. Finally, we have ended our discussion with the recent legal updates with respect to sensitive personal data or information.

1.11 FURTHER READING

- Ijlljs.in (2019), http://ijlljs.in/wpcontent/uploads/2017/02/AN_ANALYSIS_OF_PERSONAL_DATA_P

[156] White Paper on Privacy Protection in India (Vakul Sharma) <http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf>

ROTECTION_WITH_SPECIAL_EMPHASIS_ON_CURRENT_AMENDMENTS_AND_PRIVACY_BILL.pdf (last visited Nov 20, 2019).

- Elplaw.in (2019), https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf (last visited Nov 20, 2019).
- Webfoundation.org (2019), http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf (last visited Nov 20, 2019).
- Induslaw.com (2019), https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf (last visited Nov 20, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Define Personal Information?

The definition of ***"Personal information"*** is found under ***Rule 2(i),*** it has been defined as, any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

2. Define Sensitive Personal Data or Information?

Sensitive Personal Data or Information has been defined under ***Rule 3 of the 2011 Rules.*** It states that in respect of any person, the sensitive data or information is the one which consists of his information relating to:-

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;
vii. any detail relating to the above clauses as provided to body corporate for providing service; and

viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

3. What is the punishment for failure to comply with the provisions related to disclosure of information?

Section 72A of the IT Act, 2000 provides punishment for disclosure of information, knowingly and intentionally, without the consent of the person to whom the information relates, and in breach of the lawful contract as imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

4. What is recent case law with respect to the right to privacy?

The Hon'ble Supreme Court of India by its judgment in the case of ***Justice K.S. Puttaswamy (Retd.) &Anr v Union of India &Ors (W.P. (Civil) No. 494 of 2012)*****,** recognized and pronounced the right to privacy as a fundamental right which is given under the Constitution of India.

1.13 ACTIVITY

Elaborate the procedure to collect Sensitive personal data or information and to whom the information must be disclosure along with the recent cases with respect to privacy issues? (1000-1500 words)

Unit 2: Laws related to Online Defamation

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The meaning of Defamation
- Ingredients of defamation
- Online Defamation: An Indian Perspective

1.2 INTRODUCTION

Defamation is defined as "an intentional false communication, either published or publicly spoken, that injuries another's reputation or good name." Defamation includes the common law

torts of libel (involving written or printed statements) and slander (involving oral statements). Significantly, both libel, as well as slander, could be committed via Internet medium.[157]

1.3 INGREDIENTS OF DEFAMATION

Defamation is an intrinsically personal wrong. The gist of defamation is actual or presumed damage to reputation flowing from publication.[158] In other words, defamation flows from publication (or communication) of information. In traditional libel cases "publication" is generally referred[159] to as "the date on which the libelous work was placed on sale or became generally available to the public". It has the following ingredients:

a) Publication of a statement;

b) The statement makes reference to the plaintiff;

c) Statement is communicated to some person or persons other than the plaintiff himself;

d) Statement reaches the plaintiff; and

e) Statement causes actual or presumed damage to the plaintiff.

The question is, does one encounter similar 'ingredients' when defamation occurs in Internet medium? Here, the only difference is that the tort of defamation occurs when the defamatory imputation is published in electronic form, everything else remains the same.

1.4 IT ALL BEGINS WITH PUBLICATION

Publication is defined as "the action of making publicly known". In the context of the Internet, the term publication includes dissemination, transmission and storage of information or data in electronic form.

In order to construe a relationship between defamation and publication in the Internet medium, one may have to answer the following questions:

[157]Biegel, Stuart, Beyond our Control – Confronting the limits of our Legal System in the Age of Cyberspace, MIT Press, London, [2003] at p 82

[158] M, Collins, The Law of Defamation and the Internet, Oxford University Press, [2001] p 24.02

[159]*Kenneth Love v William Morrow & Co*., 193 AD 2d 583: 597 NYS 2d 424 2d Dep't. [1993]

1) When a "publication" takes place (which involves "time of occurrence");
2) How a "publication" takes place (which involves the "mode of publication");
3) Where the publication takes place (which involves issues such as "jurisdiction");
4) Who would be held responsible for the publication of the allegedly defamatory statements (ISP or the website promotor)?

1.5 WHEN?

Publication occurs when the contents of the publication, oral, spoken or written are seen and heard, and comprehended by the reader or hearer. From the point of view of the plaintiff, the process of publication is complete, when the communication reaches hi.

For example, In ***Godfrey vs Demon Internet Ltd.,***[160]the defendant ISP carried the newsgroup 'soc.culture.thai' and stored postings within that hierarchy for about a fortnight during which time the posting was available to be read by its customers. On 13 January 1997 someone unknown made a posting in the US in the newsgroup. This posting was squalid, obscene and defamatory of the plaintiff who was resident in England. On 17 January 1997 the plaintiff sent a letter by fax to the defendants, requesting them to remove the posting from their Usenet news server. The defendants could have obliterated the posting after receiving the plaintiff's request, but it remained available until its expiry on or about 27 January 1997. The plaintiff claimed damages for libel in respect of the posting after 17 January 1997 – the time when he affirmed to the ISP that the communication had indeed reached him.

Morland J. ruled:

"In my judgment, the defendant, whenever it transmits and whenever there is transmitted from the storage of its news server a defamatory posting, publish that posting to any subscriber to its ISP who accesses the newsgroup containing that posting. Thus every time one of the defendant's customers accesses 'soc.culture.thai' and sees that posting defamatory of the plaintiff, there is a publication to that customer".

[160]*Godfrey v Demon Internet Ltd,*4 All ER 342 (HC)

1.6 HOW?

How the publication has occurred, i.e., in what form (mode) publication has happened? It is an important issue in the techno-legal driven environment. It looks into the mode of publication (or transmission) – whether audio, video, textual or multimedia. Internet publishing is in 'electronic form'. Instances of defamation in 'electronic form' include generating, sending or receiving 'defamatory' e-mails, online bulletin board messages, chat room messages, music downloads, audio files, screaming videos, digital photographs etc. on the Internet.

1.7 WHERE?

Where the publication has occurred is not easy to define as a defamatory statement can be "published" anywhere in the world where there is access to the Internet. Here, the issue is whether due process of law would be served by hauling a defendant into a particular jurisdiction simply because he has posted information that can be accessed anywhere in the world.

In the context of Internet it is not necessary for the plaintiff in all cases to prove directly that the defamatory statement was brought to the actual knowledge of anyone (some person or persons other than the plaintiff himself), publication is only established if the plaintiff makes it a matter of reasonable inference that the publication was accessible in the said jurisdiction. In contrast, with the Internet, it is not at all probable that every website will be accessed in every jurisdiction where it can theoretically be accessed. So, as a matter of reasonable inference, it cannot be assumed that any site put on the Internet and theoretically accessible from anywhere is accessed everywhere. Where then can the publication be assumed to have taken place.

In ***R vs Graham Waddon,***[161] the defendant was charged with numerous counts of publishing obscene articles contrary to section 2(1) of UK's Obscene Publications Act, 1959. The defendant had created pornographic images, which were illegal under the UK's Obscene Publications Act. He ran a series of sites based in the US, hosting them on a US-based Internet service provider. These images were accessible to anyone in the world via the Internet who became a subscriber

[161] *R v Graham Waddon* Southwark (Crown Court, 30-6-1999)

by giving credit card details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could log onto the various websites to obtain the images. It was submitted on behalf of the defendant that, because the Internet publication had necessarily occurred abroad, therefore the instant court did not have jurisdiction.

Hardy, Christopher J. held:

"Publishing an article under Section 1(3)(b) of the 1959 Act included data stored electronically and transmitted. To transmit meant to send from one place or person to another. In the instant case, an act of publication took place when the data was transmitted by the defendant or his agent to the service provider, and the publication or transmission was in effect still taking place when the data was received. Both the sending and receiving took place within the jurisdiction of the court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving".

In other words, the court exercised its jurisdiction, even when the pornographic material was held on a US-based server. The court argument has been that since the material was uploaded (by Waddon) and downloaded (by the police) in the UK, it could be classified as being "published" in the UK.

In ***Dow Jones & Company IncvsGutnick,***[162] on the other hand, the High Court of Australia approved the trial court's assertion of jurisdiction over Dow Jones & Co., based on its online publication of an allegedly defamatory article. The article appeared in Barron's Online, the online version of Dow Jone's print publication Barron's, which was available to subscribers of wsj.com. Joseph Gutnick, a resident of the Australian state of Victoria, brought a defamation action against Dow Jones in a Victoria court. Dow Jones argued that the court should decline jurisdiction under the doctrine of forum non-conveniens, which would be applicable if the Victoria court was a "clearly inappropriate forum". Dow Jones argued that Barron's Online was published in New Jersey, the location of the servers hosting the wsj.com website. From this, it would follow that the substantive law to be applied in deciding the case in New Jersey law, which would make the Victorian court a inappropriate forum. Thus the decision hinged on where the article was deemed to be published.

[162] *Dow Jones & Company Inc vGutnick*[2002] HCA 56 (Austl)

The court held, contrary to Dow Jone's contention, that publication of a defamatory statement is "a bilateral act in which the publisher makes it available and a third party has it available for his or her comprehension". Therefore, the article was published, with respect to Gutnick's cause of action, not when Dow Jones placed it on its web server, but only when subscribers in Victoria accessed it. The site recorded about 550,000 hits, less than 0.01 percent of them from people with Australian credit cards. It was not ascertainable how many of these users were Victorian but it was agreed that "several hundred" downloads had taken place in Victoria. For these reasons, the court held that the defamation occurred in Victoria and that Victorian law-governed: "It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed". Since jurisdiction in Victoria was proper, and Victorian law would be applied, the Victorian court was not a "clearly inappropriate forum," and there was no basis for declining jurisdiction.

The court responded to Dow Jones's policy arguments with the observations: (1) a plaintiff can win damages only in a location where he has a reputation, which limits the choice of forum; (2) a judgment for damages is enforceable only in locations where the defendant has reachable assets; and (3) publishers can easily determine in advance which law will apply in defamation cases: the specter which Dow Jones sought to conjure up in the present appeal, of a publisher forced to consider every article it publishes on the World Wide Web against the defamation laws of every country from Afghanistan to Zimbabwe is seen to be unreal when it is recalled that in all except the most unusual of cases, identifying the person about whom material is to be published will readily identify the defamation law to which that person may resort.

The Court concluded for centuries that the law in defamation cases has been that publication takes place when and where the contents of the publication, oral or spoken, are seen and heard (i.e., made manifest to) and comprehended by the reader or hearer. Having decided that a person is defamed at the place where publication is made, the Court found that the dissemination of the material on the Internet and the downloading of that information in Victoria meant that publication had been made there.

1.8 WHO?

Who would be held responsible for the publication of the allegedly defamatory statements – the ISP or the website promoter? An Internet service provider represents an interactive network service. It may provide access to the Internet (a network of networks) only or offer a range of additional services. Depending upon its functional attributes, an Internet service provider may act as an 'information distributor (carrier)' or 'information publisher'.

An information distributor merely acts as a carrier of information (third party content) transmitting 'electronic message' from one place to another, without examining its content. The function of an information publisher is to not only publish and transmit the information but also take reasonable care in relation to the said publication.[163]

It is thus important to look into the cases, where the court has identified ISPs (or bulletin board operators) as either 'information distributor' or 'information publisher'. In ***Cubby, Incvs CompuServe, Inc.,***[164] where CompuServe is an online company providing access to over 150 special interest forums comprised of electronic bulletin boards, interactive online conferences, and topical databases. A newsletter called Rumorville was made available via the bulletin board. The plaintiff sued CompuServe for libel after allegedly defamatory statements were disseminated through the newsletter against it. Cubby argued that the court should consider CompuServe to be a "publisher" of the allegedly defamatory statements, and thus hold it liable for the statement.

1.9 ONLINE DEFAMATION: AN INDIAN PERSPECTIVE

In India, issue of defamation has so far been dealt under the provisions (Sections 499-502) of the Indian Penal Code, 1860. The Code makes no distinction between slander and a libel. It defines "defamation" as:

Section 499 states that, whoever by words, either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except[165] in the case hereinafter excepted, to defame that person.

[163]S KVerma and Raman Mittal (Ed.), Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, [2004], p 233

[164]*Cubby, Inc v CompuServe, Inc*776 F Supp 135 (SDNY) [1991]

[165] There are 10 exceptions (defences), that may be set up against a charge of defamation

The three ingredients[166] are:

1) Making or publishing any imputation concerning any person
2) Such imputation must have been made by
a) Words, either spoken or intended to be read; or
b) Signs; or
c) Visible representations
3) Such imputation must have been made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning whom it is made.

The Code also highlights that defamatory statements need to be published (or communicated). The Supreme Court held in ***Bennett Coleman & Co. vs Union of India,***[167] that "publication means dissemination and circulation". That is, communicating defamatory statements only to the person defamed is not publication.

It is important to note that an essential difference between the Indian and the English law is that the former recognizes 'words spoken' as a mode of defamation, and the latter does not. It was held by the Supreme Court in ***BalrajKhannavsMoti Ram:***[168]

"It will be highly desirable no doubt if the actual words stated to have been used by an accused and which are all to be defamatory are reproduced by the complainant. The actual words used or the statements made may be reproduced verbatim by the complainant if the words are few and the statement is very brief. But in cases where the words are spoken are too many or the statements made are too long, it will be the height of technicality to insist that the actual words and the entire statements should be produced verbatim".

The Code by highlighting that defamation could also happen by means of 'signs' or 'visible representations', has included every possible form of defamation, including defamation in 'electronic form' as well. Instances of defamation in 'electronic form' includes generating, sending or receiving 'defamatory' emails, messages, chat room messages, music downloads, audio files, streaming videos, digital photographs, tweets etc. on the Internet. Even sending

[166]Ratanlal and Dhurajlal, The Indian Penal Code, 28th Edn, P 686
[167]*Bennett Coleman & Co v Union of India*[1972] 2 SCC 788
[168]*BalrajKhanna vMoti Ram* AIR[1971] SC 1389

'defamatory' SMS, MMS, messages, photographs and videos on mobile phones would be considered instances of defamation in electronic form. In other words, the Code is sufficient in itself to tackle any online defamation matter. However, in ***ManikTanejavs State of Karnataka,***[169] it was held by the Supreme Court that:

"Facebook is a public forum; it facilitates the expression of public opinion. Posting of one's grievances against Government machinery, even on Government Facebook page does not by itself amount to criminal conduct".

Further, the Supreme Court in ***Subramanian Swamyvs Union of India,***[170] while examining the constitutional validity of Section 499 & 500 IPC has opined that "The decision in ***ShreyaSinghal case*** is placed reliance upon to highlight that a restriction has to be narrowly tailored, but criminal defamation is not a narrowly tailored concept".

1.10 LET'S SUM UP

In this chapter, we have studied the meaning and ingredients of defamation and the demarcation between defamation and online defamation. We also discussed how, when, and where online defamation commences. Finally, we ended the discussed with the Indian Perspective of Online defamation.

1.11 FURTHER READING

- Defamation on the Internet – a duty free zone after all? Uta Kohl, (2000) 22 Sydney L Rev 119, pp 126-27.
- Valdaya, Ankit, Legal Consequences of Online Defamation in India (January 28, 2014).
- Susan Singleton, Simon Halberstam, Business, The Internet And the Law, 1999, Tolley Publishers, U.K.
- Martin Samson, Online Defamation/Libel/Communications Decency Act - Internet Library of Law and Court Decisions

[169]Manik*Taneja v State of Karnataka* [2015] 7 SCC 423
[170]*Subramanian Swamy v Union of India*[2016] 7 SCC 221

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of defamation?

Defamation is defined as "an intentional false communication, either published or publicly spoken, that injuries another's reputation or good name."

2) What are the ingredients of defamation?

It has the following ingredients:

a) Publication of a statement;

b) Statement makes reference to the plaintiff;

c) Statement is communicated to some person or persons other than the plaintiff himself;

d) Statement reaches the plaintiff; and

e) Statement causes actual or presumed damage to the plaintiff.

3) What are the questions that need to be posed in order to find out the relationship between defamation and publication?

- When a "publication" takes place (which involves "time of occurrence");
- How a "publication" takes place (which involves the "mode of publication");
- Where the publication takes place (which involves issues such as "jurisdiction");
- Who would be held responsible for the publication of the allegedly defamatory statements (ISP or the website promotor)?

4) What are the ingredients of defamation as per IPC?

The three ingredients are:

a) Making or publishing any imputation concerning any person

b) Such imputation must have been made by

- Words, either spoken or intended to be read; or

- Signs; or
- Visible representations

c) Such imputation must have been made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning whom it is made.

1.13 ACTIVITY

Explain briefly the meaning and ingredients of defamation and how it is different from online defamation. Also, describe the same with relevant case laws as per the Indian perspective? (800-1000 words)

Unit 3: Body Corporate Responsibilities for Data Protection

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is meant by 'Reasonable Security Practices and Procedures'
- What are the responsibilities which need to be discharged by Body Corporates
- Can Body Corporates be held liable if the information given isn't authentic

1.2 INTRODUCTION

With the rampant use of the internet, there is an undeniable need for the protection of data that the people put up or share over the internet. This has been more firmly established by the pronouncement of judgment by the Honorable Supreme Court in the case of ***Justice K.S. Puttaswamy (Retd.) &Anr. v Union of India &Ors,***[171] which accorded the right of privacy as a fundamental right. Further, it is a recognized and a well-recognized jurisprudential principle that where there is a right, there is a duty. So in this situation, where the individuals have the right to privacy, the bodies or agencies which have the data of the individuals are under a duty to protect and restrain from the using or allowing the data to be used for any purpose other than that

[171] *Justice K.S. Puttaswamy (Retd) &Anr v Union of India &Ors* W P (Civil) No 494 of [2012]

permitted by law. In this chapter, we will focus on those duties of a body corporate that has been imposed upon them by the law with respect tothe protection of electronic data.

1.3 LEGAL DEFINITION OF CERTAIN IMPORTANT TERMS

The term ***'body corporate'*** has neither been defined under the Information Technology Act, 2000 nor under any of the Rules issued from time to time by the competent authorities which draw its validity and legal backing from the Information Technology Act 2000 (hereinafter referred to as 'the IT Act, 2000'). However, in the year 2008, certain provisions of the IT Act, 2002, were amended and amongst other provisions, ***Section 43A*** was brought in, which prescribed that the compensation has to be paid, to the provider of information, by the body corporate which possesses, deals or handles sensitive personal data or information who has a duty to implement and maintain reasonable security practices and procedures so as to prevent the information from unauthorized use, access, sharing, alteration or damage and which has failed to do so and, as a result of the unauthorized access or disclosure, certain loss has been caused. It is in the explanation part of this provision, certain terms have been defined, which sets out their meaning for the purpose of the section. It is in this part of this provision that body corporate has been defined. It states that 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

The term also defines ***'reasonable security practices and procedures'*** as those security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. Now, as the definition mentions the reasonable security practices and procedures as those practices as procedures as may be specified in law, the Central Government has framed certain Rules to regulate on these security practices and procedures drawing its validity under ***Section 43A and clause (ob) subsection (2) of Section 87 of the IT Act 2000.*** The Central Government notified these Rules in the year 2011, and they are ***called Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)***

Rules, 2011 (hereinafter referred to as 'the 2011 Rules'). Now we will look into the important amongst those guidelines. In the previous Chapter, those guidelines were discussed from the viewpoint of the provider of the information, but in this chapter, the discussion will follow the viewpoint of an organization that is collecting such information.

1.4 RESPONSIBILITIES TO BE DISCHARGED BY BODY CORPORATE

1. Responsibility of Body Corporate to provide a policy for privacy and disclosure of information.

   Under the 2011 Rules, ***Rule 4*** provides that the body corporate or any person, who on its behalf collects, receives, possess, stores, deals or handle information of provider of information, has to provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information. Such body corporate or any person on its behalf shall ensure that such policy is available for seeing to such providers of information who has provided the concerned information under a lawful contract, and such policy shall be published online on the website of the body corporate. The policy shall have following things among others:-

   i. Clear and easily accessible statements of its practices and policies; and
   ii. Type of personal or sensitive personal data or information collected under Rule 3 of the 2011 Rules; and
   iii. Purpose of collection and usage of such information; and
   iv. Disclosure of information including sensitive personal data or information as provided in Rule 6 of the 2011 Rules;
   v. Reasonable security practices and procedures as provided under Rule 8 of the 2011 Rules.

2. As mentioned under ***Rule 5 of the 2011 Rules,*** it is duty or responsibility of the Body Corporate or the person working on its behalf to obtain the consent of the provider of the sensitive personal information or data. Such consent must be regarding the purpose of usage and must be obtained before the collection of such information.
3. It is also the responsibility of the body corporate or the person working on its behalf to endure that the provider of the sensitive personal information is aware that such information is being collected, and the purpose for which the information is being collected, and the intended recipients of the information sought to be collected, along with the name and

address of the agencies collecting the information and of those who will be retaining the information.[172]

4. The body corporate is also under an obligation to collect information only for a lawful purpose, which is connected with any activity or function of such body corporate and when the collection of information is necessary for that purpose.
5. The body corporate or the person acting on its behalf which is holding such sensitive personal information or data is under an obligation to not retain the information retained for any time longer than what is required for the lawful purpose for which the information was retained or than the period which is permitted under any law for the time being in force.
6. One of the most important and basic responsibilities of the body corporate or the person who is working on its behalf is that the information shall be used only for the purpose for which it was collected and nothing more. This responsibility restricts the body corporate from the misuse of the data collected and this is a very big onus being placed on the body corporate.
7. It is the duty of the body corporate to enable the data or information providers to correct or amend the data or information given by them, when they request for the same, and so far as this is feasible. The point worth noticing here is that the body corporate or the person working on its behalf isn't responsible for the correctness or the genuineness of the data or information given or corrected, as the case may be.
8. Another important obligation of the body corporate is that before collecting the information, it or any person working on its behalf shall provide the provider of the information with an option to not provide the concerned data or information.
9. The obligation mentioned in the point above is also available at a later stage, whereby the consent is given can be withdrawn at a later stage, and thereby the body corporate or any person working on its behalf shall be duty-bound not to use such data or information in respect of which the consent has been withdrawn.
10. Under sub-rule 5 of Rule 5 of the 2011 Rules, another responsibility of the body corporate has been encapsulated. This obligation or responsibility is that of grievance redressal of establishing an authority for the said purpose. The Rule states that the body corporate shall address any discrepancies and grievances of their provider of the information with respect to the processing of information in a time-bound manner. The Rule also mandates the body

[172]<https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>

corporate to designate a Grievance Officer, and to ensure that this is known to the people, it is obligated to publish his name and contact details online on its website. The Rule also prescribes a timeframe within which the grievances must be taken care of and mentions that the Grievance Officer shall redress the grievances or provider of information expeditiously but within 1 month from the date of receipt of the grievance.

11. Another obligation on the body corporate is mentioned in sub-rule 8 of rule 5 of 2011 Rules. It states that the body corporate or any person working on its behalf shall keep the information secure as provided in rule 8. In relation to the same, rule 8 talks about 'Reasonable Security Practices and Procedures.'

    Rule 8 talks about presumption, in favour of body corporate or person acting on its behalf, in respect of security practices and procedures provided that they have implemented such security practices and standards and have a comprehensively documented information security program and information security policies. The requirement of such policies shall contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[173]

    The rule further lists down certain standards which, if complied with, are sufficient to raise the presumption above mentioned.

    - One such standard is: The International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements."
    - Any industry association or its entity, whose members are self-regulating by following any standard other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1) of Rule 8, needs to get its codes of best practices duly approved and notified by the Central Government for effective implementation.[174]

    The rule further mentions that the body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified (abovementioned) shall be deemed to have complied with reasonable security practices and procedures provided that such

[173]Rule 8: Reasonable Security Practices and Procedures <https://www.itlaw.in/rule-8-reasonable-security-practices-and-procedures/>

[174]<https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf>

standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource.

12. Regarding disclosure of information by the body corporate or any person working on its behalf, as the body corporate is responsible not to disclose the data or information to any other person or entity without the prior permission of the provider of the information, but this doesn't apply where the disclosure is a legal obligation of the body corporate.
13. In continuance of the obligation to not to disclose the information or data to any third party, another important yet interesting obligation of the body corporate is to disclose the data to the Government Agencies which are mandated under the law to obtain information which is covered under the 2011 Rules on certain grounds, and this has to be done by the body corporate without the prior permission of the provider of the information. So this rule is, in a way, an exception to the general rule that the disclosure of information can be made only after the prior permission of the provider. The grounds on which such disclosure is to be made by the body corporate to the Government Agencies include: for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. This rule, as mentioned in the one of the previous chapters is similar to one of the provisions under the IT Act which provides for similar grounds on which the governmental agencies can seek information from the entities retaining them and the latter are under an obligation to disclose the same to the concerned agencies on the orders of the authorities mentioned therein.[175]
14. Also, the disclosure of the information is mandatory for the body corporate in compliance with an order under the law for the time being in force (as per Sub-rule 2 of Rule 6 of 2011 Rules).[176]

[175]How to deal with Section 43A in a Company
<https://www.naavi.org/cl_editorial_12/edit_dec_2_sec43A_compliance_framework.html>
[176]Data Protected India | Insights | Linklaters
<https://www.linklaters.com/en/insights/data-protected/data-protected---india>

So these were the major responsibilities or obligations of the body corporate in respect of data protection, which can be ascertained from the legal regime which is existing at present.

1.5 LET'S SUM UP

In this chapter, we have studied the meaning of reasonable security practices and procedures along with certain important terms related to data protection. Finally, we have ended our discussion with the responsibilities to be discharged by body corporate.

1.6 FURTHER READING

- Privacyinternational.org (2019), https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf (last visited Nov 21, 2019).
- Ghosh, Dr. Jayanta. (2016). 'Privacy and Data Protection Laws in India: A Right-Based Analysis.
- India: Data Protection & Cyber Security - AZB & Partners, AZB & Partners (2019), https://www.azbpartners.com/bank/india-data-protection-cyber-security/ (last visited Nov 21, 2019).
- Thelawreviews.co.uk (2019), https://thelawreviews.co.uk/digital_assets/25776d4c-702f-41bb-82a0-cb3e18240506/Privacy.pdf (last visited Nov 21, 2019).

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Was 'body corporate' originally defined in the Information Technology Act, 2000?**
   No. However, Section 43A was inserted by Information Technology (Amended) Act, 2008, in the explanation of which the term 'body corporate' was defined for the first time in the law relating Information Technology.

2. **Can body corporate obtain information on the assumption that the provider of the information is aware of the purpose for which the information is to be used?**
   No, it has been mentioned under "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", that it is the responsibility of the body corporate to make sure that the provider of the information is aware of certain things, one of which is the purpose for which the information is being collected. And therefore the body corporate can't record the information or data on presuming the knowledge of the provider.

3. **Does body corporate need to obtain the prior permission of the provider of information if it is ordered to disclose the concerned information by a court's order?**

   In the situation mentioned above, since disclosing the concerned information becomes the legal obligation on the body corporate due to it coming from the court's order, hence the prior permission isn't necessary for such a situation.

4. **If the information is provided by a person with his free consent for a particular purpose, can such information be used for any other purpose for which he hasn't consented specifically?**

   The obligations as mentioned under the 2011 Rules, specify that the consent which is necessary must be for the specific purpose for which the information is to be used. Thus the information can't be used for any purpose other than that for which it was consented to.

5. **If the provider of the information has any grievance against any body corporate, whom does he need to approach, and by when shall the grievance be resolved?**

   The Body Corporate has to appoint a Grievance Officer for resolving such grievances, and it has to be done within one month.

1.8 ACTIVITY

Mention all the situations (covered under IT Act, 2000, and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011) under which the information or data can be disclosed to third parties. (800 Words)

Unit 4:Right To Be Forgotten

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The history of the right to be forgotten
- Approach of Indian Laws towards the concept of the right to be forgotten
- The Personal Data Protection Bill, 2018 in context of the right and its shortcomings

1.2 INTRODUCTION

The concept of the 'right to be forgotten' is very new and as of now, has legally found its mention only in the European Union. The best meaning which can be attributed to the term is the right of any person to restrain everyone else to publish or make known any information whatsoever regarding the former. In the Jurisprudence of Indian laws, the terms haven't been defined anywhere in any of the laws in force. However, there are certain provisions which prohibit the publishing of the names or any detail which could reveal the identity of a certain

person (majorly the rape victims). The recent and the most important thing in Indian Laws context is that the Ministry of Electronics & Information Technology under the Central Government has issued ***Personal Data Protection Bill, 2018 (hereinafter referred to as 'the 2018 Bill')***[177] which for the first time in the history of Indian Laws has dealt with the concept of the 'right to be forgotten', and that too in the field of Information Technology. This right in the form as in the 2018 Bill would be focused upon in this Chapter.

1.3 STATUS OF RIGHT TO BE FORGOTTEN VIS-À-VIS RIGHT OF PRIVACY: A THOUGHTFUL APPROACH

On a thoughtful consideration of the nature of the 'right to be forgotten', it would not be wrong to relate it with the right to privacy. To get a better understanding and to provide more clarity on the matter, let's look at it from the grass-root level. Suppose a person 'X' has provided certain information to the body corporate say 'Y', now assuming that 'X' hasn't been given the right to privacy under the laws by which he is being governed then obviously he wouldn't have the right to ask 'Y' to keep his data private and restrain from sharing it to anyone, which in essence is the whole foundation of the 'right to be forgotten' because the right is nothing more than the right to compel any person to either delete the data which he might have respecting a person or to delete such data, or in other words it is the right to ask the another to keep the information private, hence arising from the right of privacy only.[178]A very similar reasoning must have been followed in drafting the 2018 Rules, as is evident by reading the objectives to bring up the 2018 Bill. The Hon'ble Supreme Court has accorded the right to privacy a status of ***Fundamental Right, in the J. Puttaswamy case***[179]**.** Thus, it would be correct to say that the ruling, in that case, has paved the way for this right to be forgotten as well.

1.4 STATUS OF RIGHT IN THE PRESENT INDIAN LEGAL MATRIX

At present, the right to be forgotten, in whatever manner, in the present Indian laws can be ascertained by referring to certain provisions of ***Indian Penal Code, 1860 and Protection of***

[177]<https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>
[178] See EUROPEAN COMMISSION, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12) (2014),
<http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf>
[179][2017] 10 SCC 1

Children from Sexual Offences Act, 2012 and Juvenile Justice Act 2015. Looking at them individually as follows:

- Under Indian Penal Code, Section 228A, prevents any person from making known the name and identity of the victim of offences falling under 376, 376A, 376AB, 376B, 376C, 376DA, 376DB or 376E, by making it an offence to do so.
- Under the Protection of Children from Sexual Offences Act, 2012, a combined reading of Section 24(5) and Section 33(7) makes it sufficiently apparent that the name and identity of the child are not to be disclosed at any time during the course of investigation or trial.
- Under the Juvenile Justice Act, 2015, the proceedings against any juvenile are required not to be recorded. This is directed with an intention to prevent the identity of such juvenile known from others.

1.5 THE BIRTH OF THE RIGHT TO BE FORGOTTEN

For understanding more clearly the importance of the right, it would be helpful to read about the journey of the same.

- The origin of ***'Right to be Forgotten'*** can be traced back to the western countries in the year 1995. Back then, the European Union brought in force their first-ever piece of law in the field of personal data protection, which is ***'Directive 95/46/EC'.*** It is important to note that the said document didn't specifically mention the term "right to be forgotten" but the same was readily inferable when ***Article 6(1)(e) is read with Article 12(b).*** Where the prior provision refrains the data from being used for any purpose other than the one for which it was collected, whereas the latter gave the provider of the information the right to ask to rectify, erase or block the data which is found violative of this Directive 95/46/EC.
- Later, the 'Right to be Forgotten' was laid down by the European Court of Justice in the case of ***Google Spain SL v. Agencia Española de Protección de Datos& Mario Costeja Gonzalez (famously known as the "Google Spain Case").*** In the case, the European Court of Justice upheld the 'Right to be Forgotten' if the data related to him is not needed for the purpose for which it was collected.[180]

[180] RAYMOND S.R. KU & JACQUELINE D. LIPTON, CYBERSPACE LAW: CASES AND MATERIALS 117 (3rd ed. 2010)

- Then in the year 2016, ***the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as 'the GDPR')*** was drafted which came into force from 2018. It is a regulation on data protection and privacy. Under Article 17 of the GDPR individuals have the right to have personal data erased, it is this right which is also known as the 'right to be forgotten'. It has to be noted that this right is not absolute and only applies in certain circumstances. With the coming in force of the GDPS, the 'Directive 95/46/EC' has been repealed.[181]

1.6 JUDICIAL PRECEDENTS FRAMING THE WAY FOR THE 'RIGHT TO BE FORGOTTEN' IN INDIA

The 'Right to be Forgotten' as mentioned earlier isn't found on any of the laws in India, not even in the Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011. However, there are certain judicial pronouncements on the matter. The Gujarat High Court and the Karnataka High Court have taken differing stands on the 'Right to be Forgotten'. Gujarat High Court in ***DharamrajBhanushankar Dave v. State of Gujarat &Ors.***[182]denied to recognize any such right. In this case, the respondent had published a non-reportable judgment on a website which concerned the plaintiff as well, and the High Court in its judgment refused to compel the respondent to take the same down. The High Court then held that the petitioner failed to prove any violation of ***Article 21 of the Constitution of India.*** The analysis of this judgment gives an idea that the Gujarat High Court did not recognize the 'Right to be Forgotten'.

However, the Karnataka High Court in the case of ***Sri Vasunathan v. The Registrar General &Ors.***[183]recognized the 'Right to be Forgotten'. In the judgment, the High Court directed the respondent to remove the name of plaintiff's daughter as the High Court had earlier quashed the FIR against her by an order. ***Justice AnandByrareddy*** who gave the judgment in the case opined that:

"This would be in line with the trend in the Western countries where they follow this as a matter of rule "Right to be Forgotten" in sensitive cases involving women in general and

[181]Frosio, Giancarlo (2017) Right to Be Forgotten: Much Ado About Nothing. SSRN Electronic Journal. 10.2139/ssrn.3009153
[182]*DharamrajBhanushankar Dave v State of Gujarat &Ors*SCA No 1854 of [2015]
[183]*Sri Vasunathan v The Registrar General &Ors* W P No. 62038/2016

highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."

Apart from these judgments, another important order is the order of the Delhi High Court, in the case of ***ZulfiqarAhman Khan v. Quintillion Business Media Pvt. Ltd.***[184] In this case, the plaintiff was accused in ***#MeToo complaints*** and the respondents published a couple of article regarding the same which were ordered by Delhi High Court to be taken down and the court also ordered these articles not to republished by any other person also. However, another platform published those articles and thus on this issue, the court passed an order restraining the re-publication of the said articles till the time matter is pending in the Court. The Delhi High Court also said that the ***'Right to be Forgotten'*** as well as ***'Right to be Left Alone'*** are the inherent facets of ***'Right to Privacy'.***[185]

1.7 THE 2018 BILL AND THE RIGHT TO BE FORGOTTEN

Before coming to the discussion of the 2018 Bill, it is important to look at certain definitions, which will be helpful in the discussion below.

- ***Section 3(14) of the 2018 Bill,*** defines ***'Data Principal'*** as "natural person to whom the personal data referred to in sub-clause (28) relates".
- ***Section 3(13)of the 2018 Bill,*** defines ***'Data Fiduciary'*** as "any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of the processing of personal data"

The 'Right to be Forgotten' is not a settled and recognized concept of law in India but it has been incorporated under the newly drafted 2018 Bill. Section 27 of the 2018 Bill encapsulates the 'Right to be Forgotten'. It gives 'data principal' a right to restrict the disclosure of his/ her personal data by 'data fiduciary'. The Section also provides that the 'data principal' shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal on the grounds if:

(a) his personal data has served the purpose for which it was collected; or

(b) he withdraws his consent for collecting his personal data; or

[184] *ZulfiqarAhman Khan v Quintillion Business Media Pvt. Ltd* CS (OS) 642/2018

[185] <https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf>

(c) the disclosure of his personal data is in violation of any existing legislation.

However, this right would be given effect to if and when the Adjudicating Officer is satisfied that the said right overrides the Right to Freedom of Speech and Expression and the Right to Information of other citizens of India.

The next provision which relates to the matter in hand is Section 10 of the 2018 Act. It is well accepted that the 'Right to be Forgotten' does not include in itself the right to deletion of the data but Section 10 of the 2018 Bill places the obligation on 'data fiduciary' to delete the personal data which was collected, after the time during which it may reasonably be necessary for the purpose for which such data was collected. However, it may extend the abovementioned time, if the retention of the data is made any legal obligation. A careful reading of the 2018 Bill shows the intention of the 2018 bill to point out that the deletion of personal data is not a matter of right for 'data principal' but it's an obligation on 'data fiduciaries'.

Another unique feature which has been attached in exercise of 'Right to be Forgotten' under the 2018 Bill is that before the exercise of this right, an application has to be filed by the 'data principal' before the Adjudicating Officer. This is unique feature attached with this right, because such application needn't be filed before exercising any of the other rights available to 'data principal'. This feature has undoubtedly made the exercise of this right relatively time consuming.

1.8 SHORTCOMINGS OF THE 2018 BILL

Few of the shortcomings of the 2018 Bill, which can be found out are:

1. 'Right to be Forgotten' can't be given the status of an absolute right as it will do more harm than good. Under the GDPR, there is a bar on exercise of right the if the data is needed for the purpose of public interest, compliance with any legal obligation, national security, scientific and historical research etc. On the other hand, under the 2018 Bill, the restriction of the exercise of the right is given on the grounds of 'right to freedom of speech and expression' and the 'right to information' of any citizen. Thus in 2018 Bill, it

is evident that the grounds of the restrictions in the exercise of the right are narrower and do not cover other important grounds like those covered under the GDPR.[186]

2. Also, the exercise of this right in its true sense may also involve the deletion of information from private storage which isn't practically feasible and also might create a hurdle in publishing the information later on. Thus, a distinction between the deletion of information and restriction over disclosure of information would be more appropriate, and only the latter one is more feasible to be granted.
3. Under the 2018 Bill, there is a very apparent confusion about the ownership of the personal data. Regarding the deletion of the data, the 'data principal' has to apply before the Adjudicating Officer, and hence here the discretion is given to such officer, this impliedly refutes the point that the owner of the data is the 'data principal'. Further, Section 27 of the 2018 Bill gives the right to apply before review even to third parties, thus this provision also adds on to the confusion over the ownership of the data.
4. Under Section 28(2) of the 2018 Bill, 'data fiduciary' is empowered to charge a reasonable fee for complying with the request of, and, when any 'data principal' exercises the rights granted to him under the PDP Bill. The provision seems fine but the problem with it is that there is nothing in the 2018 Bill to fix the criteria for determining such fee. Such uncontrolled power is susceptible of being misused by the 'data fiduciary'.

The Bill is still a draft and hasn't been codified into an Act yet, and any shortcomings can be taken care of right now. Introducing the same changes later on would be more difficult once the Bill takes the form of an Act, and thus the concerned ministry and policy makers must take up the suggestions which have been sent in huge numbers and must incorporate the best ones so as to obtain a law which, though is certain to be a landmark but, must be such that the other nations also must look up to as an ideal law in the field.

1.9 LET'S SUM UP

In this chapter, we have studied the history of the right to be forgotten along with the status of Right to be Forgotten vis-à-vis Right of Privacy. Furthermore, we studied about the approach of Indian Laws towards the concept of the right to be forgotten. Finally, we have ended our discussion with the Personal Data Protection Bill, 2018 and the shortcomings of the bill.

[186]<https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf>

1.10 FURTHER READING

- Article19.org (2019), https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf (last visited Nov 22, 2019).
- Myers, Marcus. (2014). Digital Immortality vs. "The Right to be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy. Romanian Journal of Communication and Public Relations. 16. 10.21018/rjcpr.2014.3.175.
- Frosio, Giancarlo. (2017). Right to Be Forgotten: Much Ado About Nothing. SSRN Electronic Journal. 10.2139/ssrn.3009153.
- Scholarlycommons.law.case.edu (2019), https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1081&context=jolti (last visited Nov 22, 2019).

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Whether the 'Directive 95/46/EC' categorically recognized Right to be forgotten?**
   No. the first time this right was categorically recognized was in General Data Protection Regulation (EU) 2016/679.

2. **Whether any person can apply for the exercise of right to be forgotten?**
   No. Only the 'data principal' is entitled to apply before Adjudicating Officer for the exercise of the right dealt with under section 27 of the 2018 Rules.

3. **What are the grounds under which the 'data principal' can ask for his right mentioned under Section 27 of the 2018 Bill?**
   The grounds on which the 'data principal' can ask for exercise of his right to be forgotten are as follows:

   (a) his personal data has served the purpose for which it was collected; or

   (b) he withdraws his consent for collecting his personal data; or

   (c) the disclosure of his personal data is in violation of any existing legislation.

4. **When can Adjudication Officer refuse the 'data principal' from exercising his right under Section 27 of the 2018 Bill?**

Adjudication Officer may refuse the 'data principal' from exercising the mentioned right if the rights and interests of the 'data principal' in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen.

5. **Whether Section 228A of the Indian Penal Code, 1860, protects from disclosure the identity of the person accused of Section 377 of the IPC?**

   No, since Section 228A of the IPC specifically enlists certain provisions, and the details as to the identity of the person who are victims of those mentioned provisions only is prohibited, and Section 377 of IPC isn't one of those provisions thus it won't be covered under Section 228A of IPC. Moreover, the identity of the victims is being shielded under sections 228A and not of those who are perpetrators.

1.12 ACTIVITY

Write a note on whether the right to be forgotten shall supersede the right to know along with relevant legal backing. Also, if supporting the harmonious approach, also suggest the approach which you think would best suit the conditions of our country. (1000-1500 words)

BAOU
Education for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-81-949119-9-9