BAOU
Education for All

Dr. Babasaheb Ambedkar
Open University
(Established by Government of Gujarat)

Cyberspace and Its Governance
MSCCS-402

Master of Science
Cyber Security

2022

Cyberspace and its Governance

Dr. Babasaheb Ambedkar Open University

Cyber Space and Its Governance

Course Writer

Dr. Peter Ladis F — Faculty, Chanakya Law University, Patna, Bihar

Mr. Kumar Gaurav — Faculty, Chanakya Law University, Patna, Bihar

Content Editors

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

ISBN:

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

Dr. Babasaheb Ambedkar Open University

MSCCS-402

Cyber Space and Its Governance

Block-1
Cyberspace: Meaning and Its Development

Unit 1: Cyberspace-An Overview of the Concept

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After studying this unit, the student should be able to understand:

- The meaning of the concept called cyberspace and its different definitions.
- Get aware about different layers of cyberspace.
- The relationship of the cyberspace and the internet.
- Recent and contemporary developments of and in the cyberspace.

1.2. INTRODUCTION

Cyberspace is a unique domain that is operationally distinct from the other operational domains of land, sea, air, and space. It provides, through the Internet, the capability to create, transmit, manipulate, and use digital information. The digital information includes data, voice, video, and graphics transmitted over wired and wireless facilities between a wide range of devices that include computers, tablets, smartphones, and control systems. The Internet serves as the transport

mechanism for cyberspace. The extensive variety of content is attractive to hackers, criminal elements, and nation-states with the objective of disrupting commercial, military, and social activities.

1.3 MEANING AND DEFINITION OF THE CYBERSPACE

Oxford English Dictionary (1997): "The notional environment within which electronic communication occurs."

Merriam-Webster Third New International Dictionary (2002): "The on-line world of computer networks."

Cambridge Academic Content Dictionary: "an electronic system that allows computer user around the world to communicate with each other or to access information for any purpose."

Cyberspace has been in our lexicon for over two decades now. William Gibson used it to describe "a consensual hallucination" in his science fiction novel, *Neuromancer (1984):,* when he sought a name to describe his vision of a global computer network, linking all people, machines and sources of information in the world, and through which one could move or "navigate" as through a virtual space.

The word ***"cyber",*** apparently referring to the science of cybernetics, was well-chosen for this purpose, as it derives from the Greek verb ***"Kubernao",*** which means "to steer" and which is the root of our present word "to govern". It connotes both the idea of navigation through a space of electronic data, and of control which is achieved by manipulating those data.[1]

Cyberspace represents the new medium of communication, electronic communication, which is fast and replacing the more traditional methods of communication. The physical objects of traditional communication are being superseded by new electronic objects. Just as physical objects exists in physical space, so do these cyber objects exist in cyberspace.2Cyberspace is a metaphor because it identifies the region where electronic communication occurs as being a kind

of space. We can analyze it using the terminology of I. A. Richards: "vehicle" and "tenor." The vehicle, or actual term used for the metaphor, is a combination of the morphemes "Cyber" (a trade name for computers which has become generalizable to all things computer related) and "space" (which covers a lot of territory: outer-space, inner-space, euclidean-space, non-euclidean-space, and others). The tenor, or underlying situation referred to in the metaphor, is the strange but real region created within an electric network of telephones and computers. Author Bruce Sterling refers to cyberspace as not exactly "real," but being a genuine place where things happen with actual consequences. Careers are made in cyberspace, thieves' prowl in cyberspace; increasingly complete records of our lives are stored in cyberspace.[3]

1.4.LAYERS OF CYBERSPACE

In order to understand the concept of cyberspace, one way to do so is to conceptualize cyberspace in terms of multiple interdependent layers of activities. There are varied conceptualizations of the different numbers and names of layers present in current academic discourse. However, the four-layer model of cyberspace can be considered as the best way to define cyberspace.[4]

1. The Physical layer contains all the hardware devices, which include routers, switches, storage media, satellites, sensors, and other technical conduits, both wired and wireless. The physical infrastructure can be located geographically in "real space" and is thus subject to different national jurisdictions. If it were removed, the overlying layers would disappear as well, as happened in 2011 in Armenia, were reported 90% of all Internet services crashed due to a retired 75-year-old woman who single-handedly sliced through an underground fiber optic cable with her spade.

2. The Logical Layer generally refers to the code, which includes both the software and the protocols incorporated within that software. Generally speaking, a protocol defines the rules or conventions necessary to obtain a certain goal (e.g., communication). Formalizing a protocol makes it a standard. Software, in contrast, is the computer program that implements these

protocols. In this respect, protocols "are not considered to be satisfactory standards until interoperable independent implementations [within different computer programs] have been demonstrated. (This is the embodiment of the "running code" slogan.)" Networking protocols are commonly segmented by their function, and how close (or how far) away they work from the "end-user"—the average computer user. In the most common of segmentation, known as the OSI Model, basic everyday client-side applications (such as Windows Internet Explorer) operate at the top of the model (level 7), while the aforementioned TCP works on Level 4 (the Transport layer) and IP work on Level 3 (the Internet layer). Built upon the Web, for instance, more complex applications often combine certain aspects of services, which can be eventually combined and applied by other applications on even higher levels. This flexibility presents inexhaustible possibilities to create new services, which, today, include search engines, Weblog, social networking sites, podcasts, Internet telephony, Web mapping, etc.

3. The Content/Information Layer describes all the information created, captured, stored and processed within cyberspace. Information is defined as "knowledge concerning objects, such as facts, events, things, processes, or ideas". It contains all human-readable messages delivered by social media Websites or email; content of articles and books kept on memory sticks and virtual databases; news broadcasted via blogs and Websites; and music, movies and pictures consumed online. However, access to information can also be systematically limited. Blocking or removing online content from the Web happens for reasons such as protecting intellectual property rights, securing national order or social identity.

4. The Social Layer is made up of all the people using and shaping the character of cyberspace. It is the actual Internet of people and potential relationships, rather than the implied Internet of hardware and software. Essentially, the social layer includes governments as well as private sector, civil society and technical community actors. However, all share a specific characteristic: while in "real" life (extra cyberspace) people can ultimately be identified by their unique DNA code, attribution is much more difficult on the Net (intra cyberspace).[5]

1.5 CYBERSPACE VERSUS INTERNET

Cyberspace is nothing more than a symbolic and figurative space that exists within the scope of Internet. It can be said that anything that is done via the use of Internet, occurs within the confines of the cyber-space, whether that is sending an e-mail, a website, or playing a game, all of these things exist within the cyber-space.Internet, on the other hand, is a network of networks, what that means is that it is a global network that is creating by linking smaller networks of computers and servers. This network allows users to share information and other data from one point to another. The data can be in the form of text, image, or video.[6]

Cyberspace does not exist physically, except in the countless miles of electronic circuitry, fiber optic cables and silicon chips which make up our computers and our networks. Cyberspace, by its very nature, is everywhere and nowhere at once; it is the everythingness and nothingness of William Gibson's matrix. Cyberspace is an infinite, universal space, achieved by technology inhabiting a minimal amount of physical space.[7]

But immersive cyberspace as mediated through virtual interfaces, unlike the infinite reaches of physical space, is nothingness. It is a blank, black void until an artificial context is introduced. It is nothing, placeless and indescribable. The void of cyberspace has no gravity and no micro or macroclimate of Sun, wind, earth and water. In cyberspace even a horizon is artificial. There are no building codes, no monetary budgets and no neighbours in cyberspace.[8]

Internet is a network of networks, what that means is that it is a global network that is creating by linking smaller networks of computers and servers. Cyber-space is nothing more than a symbolic and figurative space that exists within the scope of Internet.There is a lot of confusion between the usage of the terms, Cyberspace and Internet. Many people think that the words mean the space, while others think that they mean two completely different things within the field of technology. The truth of the matter is that it is something in the middle. The terms do mean two different things, but the confusion arises due to the fact that these things are closely interrelated, due of which they are often mistakenly used interchangeably.[9]

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes since then. The origin of the Internet devised from the concept of Advanced Research Project Agency Network (ARPANET). ARPANET was developed by the United States Department of Defense. Basic purpose of ARPANET was to provide communication among the various bodies of government. Initially, there were only four nodes, formally called Hosts. In 1972, the ARPANET spread over the globe with 23 nodes located at different countries and thus became known as the Internet. By the time, with the invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripts languages etc. Internet provided a medium to publish and access information over the web.

Internet covers almost every aspect of life, one can think of. Let us discuss some of the advantages and disadvantages of the internet:

ADVANTAGES:

- The Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the web that uses the Internet as a medium for communication. One can find various social networking sites such as:
    - Facebook
    - Twitter
    - Yahoo
    - Google+
    - Flickr
    - Orkut
- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.
    - Online Television

    - Online Games
    - Songs
    - Videos
    - Social Networking Apps
- The Internet allows us to use many services like:
    - Internet Banking
    - Matrimonial Services
    - Online Shopping
    - Online Ticket Booking
    - Online Bill Payment
    - Data Sharing
    - E-mail
- The Internet provides the concept of **electronic commerce** that allows the business deals to be conducted on electronic systems.

DISADVANTAGES

- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
- Another disadvantage is **Spamming**. Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of the entire system.
- **A virus** can easily be spread to the computers connected to the internet. Such virus attacks may cause your system to crash or your important data may get deleted.

- Also, the biggest threat on the internet is pornography. There are many pornographic sites that can be found, letting your children use the internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

From the above discussion it can be said that now internet is a social phenomenon that has transformed many aspects of daily life. However, one cannot separate the internet and cyberspace from each other, they cannot be independent of each other. Their interrelationship will further be elaborated in different chapters.

1.7. LET'S SUM UP

In this chapter we tried to explore the concept of cyberspace by first discussing the different definitions available. The term first appeared in the fiction novel which now represents a virtual place which is both real and artificial at the same time. With introduction of internet it can be said that it has opened new medium of communication, a global space inhabited everyday. To further understand the concept we discussed the four different layers of cyberspace and how these layers carried different framework and functions. We touched upon the numerous changes that took place regarding cyberspace till date. In brief we have discussed relationship of internet and cyberspace, how they supplement and complement each other. The characteristics of cyberspace will be discussed in the next chapter in order to have in-depth understanding of the concept of cyberspace.

1.8 FURTHER READING

- http://pespmc1.vub.ac.be/CYBSPACE.html
- https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSPExports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210
- https://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_-_Working_Paper_65_2.pdf

- See, for instance, Martin C. Libicki, *Conquest in Cyberspace. National Security and InformationWarfare*(Cambridge: Cambridge University Press, 2007). Chapter 10.; and Franklin D. Kramer, StuartH. Starr, and Larry Wentz, eds., *Cyber Power and National Security* (Washington, DC: NationalDefence UP, 2009), Chapter 2.
- https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html
- https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Q. 1 What do you understand by 'cyberspace'?

A. It is the virtual space that allows navigations for the purposes of electronic communication through a medium using computers, computer network and their users.

Q. 2 What are the various layers of cyberspace?

A. The various layers of cyberspace are i) Physical Layer, ii) Logical Layer, iii) Content Layer and iv) Social Layer.

Q. 3 What are the disadvantages associated with cyberspace?

A. The disadvantages associated with cyberspace *inter alia* include that it involves scope of spamming, virus infection, exposure to pornography, identity theft, etc.

Q. 4How is cyberspace different from the internet?

A. Cyberspace is different from the internet because while the former is the network of networks interlinking devices and servers, the former only forms a symbolic space which does not exist physically but figuratively forms a part of everything going on in the internet.

1.10 ACTIVITY

Write an essay on the concept of cyberspace with special focus on its emergence, growth and its comparison with the internet. (800 words)

Unit 2: Inherent Characteristics of Cyberspace

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After studying this unit, the student should be able to understand:

- The inherent characteristics of cyberspace
- Impact of the borderless phenomenon on regulation
- Know the pros and cons of anonymity feature cyberspace
- Realization of challenges posed by the speed of cyberspace
- Analyse the significance of Interconnectedness and Surveillance feature of cyberspace.

1.2. INTRODUCTION

The Internet is the newest form of communication between organizations and people in modern society. Everyday commerce depends on it, and individuals use it for social interactions, as well

as for reference and learning. Discoveries, Inventions and spread of new Information Technologies brought about by computers, internet and cyberspace widen the scientific horizon but pose new challenges and created problems for the legal world in all aspects of the law. [10]Cyberspace provides opportunities for innovation, commerce, and societal advancement but also raises significant issues for policymakers in securing cyber vulnerabilities, ensuring privacy and protection of personal data, and considering the use of cyberweapons as a national security asset. Cyber threats pose a broad and deep challenge. Over the past decade, governmental and non-state hackers have become increasingly sophisticated in their assaults on the cyber systems the nation depends on essential services, economic prosperity, and security. [11]Such breaches threaten critical infrastructure, intellectual property, privacy of users' data, sensitive national security information, and government personnel data. Future cyber-attacks could threaten the interconnected global economy and raise the prospect of cyber warfare between nation-states. The Internet is also being used for other malign purposes—by criminals to operate their nefarious enterprises and by terrorists to recruit and encourage violent attacks through online propaganda. If we analyze the challenges then we come to know that seed of these complications lies in inherent characteristics of cyberspace i.e. cyberspace is a borderless phenomenon, a feature of anonymity in cyberspace, lightning speed of cyberspace and interconnectedness along with surveillance characteristics of cyberspace.

1.3. BORDERLESS

Cyberspace is a borderless phenomenon. It defies the geographical territories and that is why it has been said that in the regime of cyberspace geography became history. Distance is dead in cyberspace. In this web shrink world, anyone can visit any destination virtually. It turned the word in a small village which is interconnected through various computer networks distributed worldwide. This borderless phenomenon is a double-edged sword because this feature of cyberspace can be exploited by both a netizen as well as the cyber offender. This creates a serious threat to the jurisdictional aspect of cyberspace which is the most complex legal issue of cyberspace.In the cyberspace, there is no geographical boundary. It establishes immediate long-

[10] Neeta Pramod, 'A study of formation and challenges of electronic contract in Cyberspace' <http://www.legalservicesindia.com/article/1943/A-study-of-Formation-and-challenges-of-electronic-contract-in-cyberspace.html>

[11]MarttiLehto and PekkaNeittaanmäki , *Cyber Security: Power and Technology* (3rd Edition, Springer 2018) 334

distance communications with anyone who can have access to any website. [12]Jurisdiction is the authority of a court to hear a case and resolve a dispute. The issue of Jurisdiction is highly conflicting and debatable in cyberlaw as to the maintainability of any suit which has been filed. [13]It becomes more complicated largely on account of the fact that the internet is borderless. The notion of jurisdiction is rooted in territoriality from the point of view of both the court which can properly assert jurisdiction and from the point of view of the law that should be applied while deciding the dispute. [14]In domestic transactions, a court will always have the jurisdiction to enforce their respective laws within their physical, geographical and political boundaries but the enforcement issues throw up several challenges when it comes to international transactions due to constant change in technology in borderless cyberspace

1.4. ANONYMITY

Anonymitycan be defined simply as being without a name or with an unknown name.[15]***Pseudonymity***is the use of a false name. Anonymity is derived from the Greek word **ανωνυμία**, meaning without a name or name-less. In colloquial use, the term typically refers to a person and often means that the personal identity or personally identifiable information of that person is not known. [16]More strictly, and in reference to an arbitrary element (e.g. a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous". [17]

Anonymity in cyberspace is a major concern for the global community. The introduction, growth and utilisation of information and communication technologies (ICTs) have been accompanied by an increase in criminal activities. With respect to cyberspace, identities are easily cloaked in anonymity. [18]Once a message sender's identity is anonymous, cyberspace provides the means to

[12]SuneetDwivedi, 'Jurisdiction Issues in Cyber Crime' (AcademiaEdu, 20-07-2007) <https://www.academia.edu/3700800/CYBER_CRIME_JURISDICTION>
[13]Vakul Sharma, *Information Technology Law and Practice* (3rdEdn. 2011 Universal) 567
[14]SubhajitBasu, '*Policymaking, Technology and Privacy in India'*, 2010 Vol II Indian Journal of Law and Technology
[15]Seymour Bosworth, M EKabay and Eric, Computer Security Handbook – I (5TH EDN. 2009 Wiley) 778
[16]Ibid
[17]Jacob van Kokswijk, *Digital Ego: Social and Legal Aspects of Virtual Identity* (5thEdn. 2007 Eburon)
[18] Mohammed Chawki, '*Anonymity in Cyberspace: Finding the Balance between Privacy and Security*', (Droit-Tic, Juill. 2006)<http://www.droit-tic.com/pdf/Anonymity_Cyberspace.pdf.>

perpetrate widespread criminal activity to the masses, with little chance of apprehension.[19] On the other hand, anonymity in cyberspace allows whistle-blowers and political activists to express opinions critical of employers and the government enables entrepreneurs to acquire and share technical information without alerting their competitors and permits individuals to express their views online without fear of reprisals and public hostility. [20]On this basis, the question of whether a State or a government can create a narrowly-tailored restriction on cyberspace anonymity without violating the privacy remains unresolved.

Anonymity often considered a cornerstone of democracy, is easier to attain than ever before, due to the recent emergence of cyberspace. Cyberspace allows people to share ideas over great distances and engage in the creation of an entirely new, diverse, and chaotic democracy, free from geographic and physical constraints. Due to the nature of ICTs, identities in cyberspace are easily cloaked in anonymity. With this anonymity, cyberspace provides the means to perpetrate widespread criminal activities with little chance of apprehension.[21]

Taking a look from another perspective, anonymity in cyberspace allows whistle-blowers and political activists to express their opinions critical of employers and further the government aids and enables the entrepreneurs in acquiring and sharing technical information without alerting their competitors and permits individuals to express their views online without fear of reprisals and public hostility. It has been made clear that in various parts of the world people may have an interest in not being identified and thus connected to certain published views and opinions. Due to the international character of the Internet, those reasons for anonymous communications which are related to the "freedom of expression" may gain new dimensions.

Before the advent of the information age, a person's identity, and information relating to his or her identification has always been controlled. But all that has changed. The advent of the information society has increased the need for identifying mechanisms and thus in turn, the public availability of the relevant technologies. Names, addresses, e-mail addresses, photographs, social security numbers, etc., are freely available on the Internet and numerous

[19] George F. du, *Criminalization of True Anonymity in Cyberspace*, Michigan Telecommunications and Technology Law Review 7 1 2001

[20]Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan and SapnaTyagi, 'Cybercrime, Digital Forensics and Jurisdiction'(4thEdn. 2011 Springer) 345

[21]Supra at 19.

identity-related characteristics are for sale. The development of ICTs makes more and more people reluctant to reveal their true identity. In combination with this, different services have recently been developed which make Internet activities, such as surfing anonymous. Facilities are also anonymous. Hence, anonymous communication is promoted as the solution to the problem. However, anonymous raises various legal questions: What exactly do we mean by anonymity? Why would people want to communicate and transact on an anonymous basis? What are the practical and legal constraints upon anonymity when communicating and transacting with others? Finally, total anonymity may be possible through the use of privacy-enhancing technologies.

1.5 TYPES OF ANONYMITY

There are two different types of anonymity: true and pseudo-anonymity. However, many scholars fail to address the distinction between these types. In this article, we will distinguish between true and pseudo-anonymity, two completely different forms of expression, with differing degrees of political and social values.

- **TRUE ANONYMITY**

This kind of anonymity is not traceable. The only coincidence or purposeful self-exposure will bring the identity of the mystery sender to others; the identity of a person acting in a truly anonymous manner cannot be definitively discovered through any amount of diligence. Some attempts can be made to discover the identity of the sender through inference, but any concrete trail of clues betraying the message sender has been erased by circumstance, the passage of time, or by the sender himself. Although a few of the forms of truly anonymous communication, such as political speech, are considered valuable, this form of anonymity has exceptional potential for illegal acts because the message senders cannot be held accountable for their actions.

- **PSEUDO-ANONYMITY**

Communications are inherently traceable in pseudo- anonymity. This kind of anonymity has significant benefits; it enables citizens of a democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions should the need somehow arise. Although this allows scope for the governments to

misuse their ability to uncover the identity of people acting pseudo – anonymously, it is not in the government's interest to break that trust; by respecting pseudo-anonymous identities, governments can often avoid the far more dangerous abuses stemming from true anonymity.

1.6 SPEED

Speed has been one of the fastest evolving features of cyberspace and this speed can be understood to have two dimensions: first as an instant mode of transaction and second the expansion of the internet itself.

Speed, as an instant mode of communication, has made our life easier and faster in comparison of earlier modes of communication. The computers process data at an extremely fast speed, at millions of instructions per second. In a few seconds, a computer can perform such a huge task that a normal human being may take days or even years to complete. The unit of speed of a computer is MHz (Megahertz) i.e. one million instructions per second. At present, a powerful computer can perform billions of operations in just one second.

The other dimension of this speed is the expansion of cyberspace itself since its beginning. The Oxford dictionary defines expansion as – enlargement of scale; anything spread out; to increase in size or effect.[22]Changes in cyberspace are driven in large part by private industry research and development. The interdependency and innovation of civilian economic markets and communications industries have a direct impact on cybersecurity.

Further, the domain itself is growing and evolving as information technology and the market expands and develop. This shapes many aspects of cyberspace and drives towards a system that allows for rapid innovation.

Why does cyberspace seem to change so quickly, presenting opportunities and challenges at a greater speed than we are accustomed to in the physical world? There are a number of reasons for this change, and they are scattered throughout the twentieth century. Steady advances in technology led Gordon Moore (co-founder of Intel) to state his belief that engineers would be able to double the number of transistors on a computer chip every two years. This observation,

[22] Oxford's English Language Dictionary (18th Edn. 2018 997)

known as Moore's Law, was made in 1975 and has held true for the past four decades. It means that the speed—processing power—of computer chips increases steadily, making laptops more powerful, turning Smartphone into handheld computers, and allowing Google searches to be completed ever-faster. Squeezing more transistors onto a chip means greater speed, and speed underpins the digital world.

The World Wide Web was invented in the year 1989. Today there are more than 1.2 billion websites. There are 3.8 billion Internet users in 2017 (51% of the world's population of 7 billion), up from 2 billion in 2015. Cybersecurity Ventures predicts that there will be 6 billion Internet users by 2022 [23](75% of the projected world population of 8 billion) — and more than 7.5 billion Internet users by 2030 (90% of the projected world population of 8.5 billion, 6 years of age and older).

With more than 460 million internet users, India is the second-largest online market, ranked only behind China. [24]By 2021, there will be about 635.8 million internet users in India. Despite the large base of internet users in India, only 26 percent of the Indian population accessed the internet in 2015. [25]This is a significant increase in comparison to the previous years, considering the internet penetration rate in India stood at about 10 percent in 2011. Furthermore, men dominated internet usage in India with 71 percent to women's 29 percent.

This statistic provides information on the number of internet users in India from 2015 to 2023. In 2018, India had 483 million internet users. [26]This figure is projected to grow to 666.4 million internet users in 2023. Despite the untapped potential, India already is the second-largest online market worldwide. The majority of India's internet users are mobile phone internet users, who take advantage of cheap alternatives to expensive landline connections that require desktop PCs and infrastructure. As of 2016, India had 320.57 million mobile phone internet users and

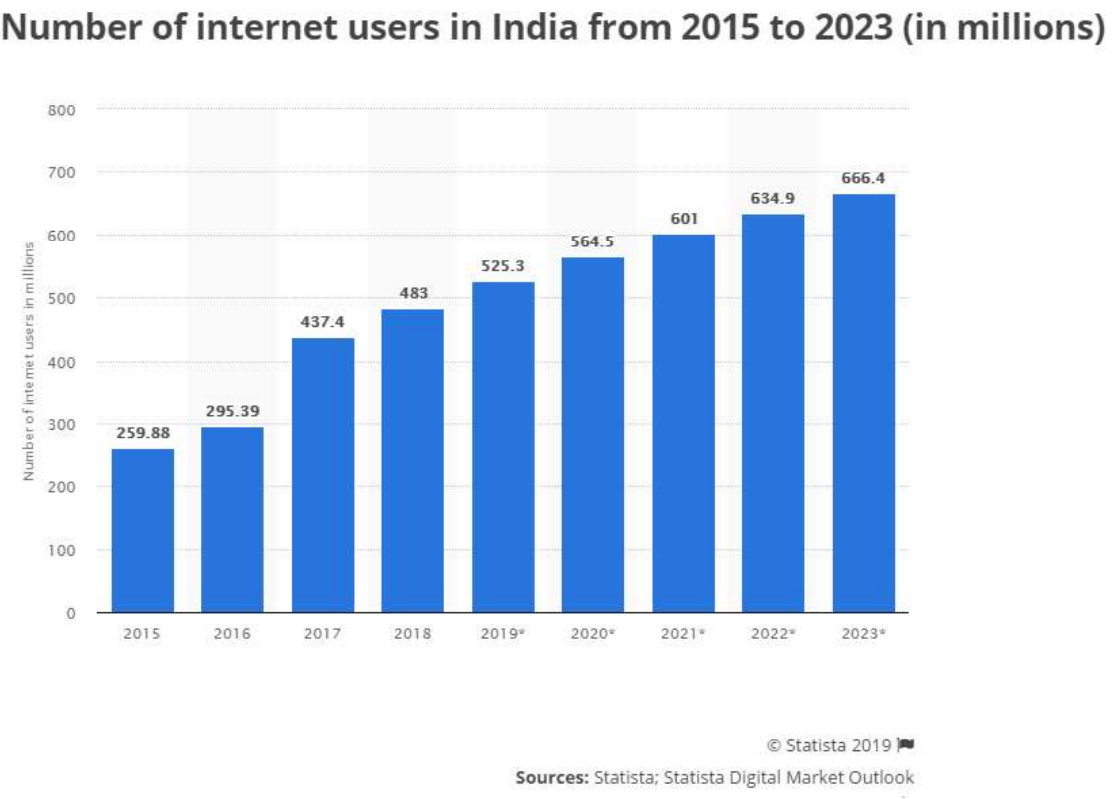
[23] Steve Morgan, '*2017 Cybercrime Report'* (2018 Cyber Security Ventures) <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>

[24]Statista Research Department, Internet Usage in India- Statistics and Facts (March 31, 2020 Statista.com) <https://www.statista.com/topics/2157/internet-usage-in-india/>

[25] Ibid

[26] Supra at 24

forecasts estimate 492.68 million Indian mobile phone internet users by 2022.[27]



1.7 INTERCONNECTEDNESS

The world is moving into space where everything and everyone is connected. This technological convergence has brought about numerous changes in our day-to-day innovation for businesses. This convergence has grown stronger over time and technological dependence has increased to such a great extent that, today, we rely on some or the other form of technology for almost any aspect of our entire life. Today, business ecosystems have become an expanded universe of intelligent devices that are interconnected, indirectly or directly, via the Internet.

The Oxford dictionary defines inter as – a prefix meaning between or among and Connectivity as – the characteristic of, or suitability for, being connected, to make connections. Cyberspace comprises of interconnected physical systems that have a host of connections within the physical

[27] Supra at 24

domain. [28]The physical systems may differ in detail, but they share the common feature that they are the foundation for the next physical system connected to them. The air domain is a physical entity and airpower relies on individual systems such as platforms, bases, logistics and personnel to function as a system of systems. In contrast, the cyber domain itself is a system of systems due to the inter-connectivity of a multitude of physical systems.[29]

It is this inter-connectivity that defines cyberspace and has allowed applications like Facebook to grow to have over 700 million users in a short span of time. This aspect of the cyber domain makes it intricate, complex to define and difficult to understand. This is compounded by cross jurisdictional boundaries and attribution difficulties that provide challenging doctrinal, legal and operational implications.

Individuals as well as corporations might have ownership of some physical systems and interconnections but there is no ownership of cyberspace as a collective. This is a quality shared with the space domain noting that entry into the cyber domain is obtained at a significantly lower cost and sophistication than into space. Users of cyberspace exploit low-entry costs, widely available resources and a minimum required investment to influence the domain.

1.8 SURVEILLANCE

Global security concerns, acts of terrorism and organised crime activity have motivated nation-states to delve into implementing measures of mass surveillance in cyberspace, the breadth of which was partly revealed by the whistleblower Edward Snowden.[30]

The vast majority of computer surveillance involves the monitoring of data and traffic on the internet in the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law

[28] Oxford's English Language Dictionary (OUP 17TH Edn 898)
[29] Air Power Centre Bulletin. 'What is Cyberspace?' (Vol 157, June 2011) <https://vdocuments.mx/what-is-cyberspace-examining-its-cha-what-is-cyberspace-examining-its-characteristics.html>
[30] Theo Tryfonas, *Human Aspects of Information Security, Privacy, and Trust* (Vol. 9750, Publisher: Springer International)201-211

enforcement agencies. [31]Packet capture is the monitoring of data traffic on a computer network. Computers communicate over the Internet by breaking up messages (emails, images, videos, web pages, files, etc.) into small chunks called "packets", which are routed through a network of computers, until they reach their destination, where they are assembled back into a complete "message" again. Packet Capture Appliance intercepts these packets as they are travelling through the network, in order to examine their contents using other programs. [32]Packet capture is an information-gathering tool, but not an analysis tool. That is it gathers "messages" but it does not analyze them and figure out what they mean. Other programs are needed to perform traffic analysis and sift through intercepted data looking for important/useful information. Under the Communications Assistance For Law Enforcement Act, all U.S. telecommunications providers are required to install packet sniffing technology to allow Federal law enforcement and intelligence agencies to intercept all of their customers' broadband Internet and voice over Internet protocol (VoIP) traffic.

A large amount of data gathered from packet capturing requires surveillance software that filters and reports relevant information, such as the use of certain words or phrases, the access of certain types of web sites, or communicating via email or chat with parties. Agencies, such as the Information Awareness Office, NSA, GCHQ and the FBI, spend billions of dollars per year to develop, purchase, implement, and operate systems for interception and analysis of data. Similar systems are operated by Iranian secret police to identify and suppress dissidents. The required hardware and software was allegedly installed by German Siemens AG and Finnish Nokia.[33]

In India surveillance by the law enforcement authorities has always been an accepted practice, in fact, it was in the context of police surveillance that the two most landmark decisions on the right to privacy were pronounced by the Supreme Court. [34]Even in those two cases, one upheld the surveillance activities of the police and the other struck them down mainly on a technical ground that they were being carried on without the proper authorizations. In the modern age, however, most surveillance activities are carried on through tapping or interception of telecommunication

[31]Maddox Howe, Management of Sports and Physical Education (5thEdn EDTECH Press 2020) 351

[32]Riley Witt, Women Education in 21st Century (3rdEdn.EdTech Press 2019) 561
[33]Skylar, Vocational Education (2ndEdn.EdTech Press 2020) 91
[34] CIS India, State of Cyber Security and Surveillance in India (2018 CIS India.org) <https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf>

messages and therefore the two most important legislations in the context of surveillance today are the Indian Telegraph Act, 1885and the Information Technology Act, 2000.[35]

The Information Technology Act, 2000 ("IT Act") widely regulates the interception, monitoring, decryption and collection of information of digital communications in India. [36]More specifically, section 69 of the IT Act empowers the Central Government and the state governments to issue directions for the monitoring, interception or decryption of any information transmitted, received or stored through a computer resource. Section 69 of the I.T. Act expands the grounds upon which interception can take place as compared to the telegraph Act. [37]As such, the interception of communications under Section 69 is carried out in the interest of:

- The sovereignty or integrity of India;
- Defense of India;
- Security of the State;
- Friendly relations with foreign States;
- Public order;
- Preventing incitement to the commission of any cognizable offense relating to the above; and
- For the investigation of any offense.

It must be noted that although the grounds for interception are roughly the same as the telegraph Act (except for the condition of prevention of incitement of only cognizable offences, defense of India and the addition of investigation of any offence) the IT Act does not have the overarching condition that interception can only occur in the case of public emergency or in the interest of public safety. Additionally, section 69 of the IT Act mandates that any person or intermediary who fails to assist the specified agency with the interception, monitoring, decryption or provision

[35] National Research Council, Engaging Privacy and Information Technology in Digital Age (20th Report 2019 NRC) 567

[36] IT Act 2000

[37] IT Act 2000, s 69

of information stored in a computer resource shall be punished with imprisonment for a term which may extend to seven years and shall bailable for a fine.

1.9 LET'S SUM UP

In this chapter, we have studied the inherent characteristics of cyberspace. We have started with the concept of cyberspace, and then we have inherent characteristics of cyberspace. We have seen how these inherent characteristics are the biggest strength as well as the biggest weakness of this cyberspace. We have also discussed the impact of these features on our day to day life.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Q. 1 What are the inherent characteristics of cyberspace?

A. The inherent characteristic of cyberspace inter alia include: borderlessness, anonymous, speedy, interconnectedness, vigilant etc.

Q. 2 How is the interception and decryption of digital communication in India done?

A. The interception, decryption, monitoring and collection of digital communication is done in India as per the provisions of the Information Technology Act, 2000 enlisted under section 69 which states that interception can take place in the interest of protection of the sovereignty, defence of the country, security of the state, establishing friendly relations with neighbouring states, maintaining public order, investigating for offences, etc.

Q. 3 What are the kinds of anonymity associated with cyberspace?

A. The kinds of anonymity associated with cyberspace are true anonymity and pseudo anonymity.

Q. 4 What does the 'borderless' phenomenon of cyberspace signify?

A. Use of cyberspace defies geographical boundaries, for distance is dead in cyberspace. Hence, cyberspace is called a borderless phenomenon.

Q 5. What is the advantage of the anonymity of Cyberspace?

A. The major disadvantage of anonymity of cyberspace lies in the fact that it does not allow easy detection of the user of such cyberspace.

1.11 FURTHER READING

- https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
- https://www.statista.com/topics/2157/internet-usage-in-india/
- http://airpower.airforce.gov.au/APDC/media/PDF-Files/Pathfinder/PF157-What-is-Cyberspace-Examining-its-Characteristics.pdf
- http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1428&context=law_lawreview
- http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1380&context=californialawreview

1.12 ACTIVITY

Write an essay capturing the inherent characteristics of cyber law, thereby throwing light on the advantages and disadvantages of its usage. (800-1000 words)

Unit 3: Forms of Cyberspace Regulations

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After studying this unit, the students should be able to understand:

- The need for regulation of cyberspace
- Aware of different modules of cyberspace regulation
- Analyze the pros and cons of each regulatory theories of cyberspace
- To know the most feasible option for cyberspace regulations.

1.2. INTRODUCTION

There have been arguments advocating that cyberspace should not be regulated and that any control in the form of regulation would stifle an unfettered potential for growth. This view arose

in response to a cumbersome web of local and national legal regimes, which added more confusion than a certainty to the cyber world. Such arguments claim that over time cyberspace will mature and so will its audience, creating a robust and socially cohesive system. These arguments, however, have little foundation.

Regulation refers to the conduct of the individual or institution to be regulated. Thus regulation encompasses three components: (1) legislation – where rules are defined, (2) enforcement – where appropriate actions are initiated against the rule violaters, and (3) adjudication – where consideration is made if the rules had indeed been breached, and where the appropriate sanctions for such breach are determined. [38]The goal of regulation is the prescription of behavioural norms. There is a great diversity of regulatory models and the norms can be divided into four categories according to their scope of application: the object, the ‘‘author, the subject and the sanction of the norm.

Regulation is necessary in Cyberspace as, without it, evidence has indicated that the cyber world will be subsumed in uncertainty and become rampant with abuse. The following example of privacy illustrates this clearly. Unregulated, cyberspace is a brutal environment, where users' rights are virtually non-existent and the remedies are confused and uncertain. An unregulated Cyberspace has the capacity to undermine entire legal systems, tear at community values and stifle commercial activity. The real purpose of this module is to stress the need for regulation of Cyberspace and the possibility and scope of its regulation.

1.3. GOVERNMENT REGULATIONS

Government regulations module is one of the prominent form of regulation where the government is regulating the affairs of cyberspace through its machinery. The legislation is one of the most significant mechanisms through which the government is regulating cyberspace worldwide. This regulation takes two forms: enforcing laws of general applicability in cyberspace and creating new laws to govern cyberspace. The adaptation of the UNCITRAL model of e-commerce for the formation of cyber laws in India is one of its examples that how Indian government framed the Information Technology Act 2000. This act also amended existing

[38]R Y COng, 'Mobile Communication and Protection of Children' (Leiden University Press 2011) 45

laws such as the Indian Penal Code, 1860, Indian Evidence Act, 1872, Bankers Book of Evidence etc. this legislation addressed various legal concerns such as legal recognition of electronic documents, recognition of electronic authentication mechanism, jurisdictional concerns of cyberspace and regulation of cyber offence and cyber contraventions. Sometimes court intervention becomes essential to regulate the affairs of cyberspace as well as deficiencies of cyberspace. The best illustration of judicial intervention can be found in the case of ***ShreyaSinghalvs Union of India***[39] which held '***section 66 A unconstitutional because it violates freedom of speech and expression in cyberspace which is one of the fundamental right enshrined under Indian constitution'.***

Although still there are some grey areas in this regulatory module. In cyberspace, distance is measured in nanoseconds - not miles. Social interaction or commercial transactions on a transnational level are possible with ease here to fore only imagined by science fiction writers who dreamed of teleportation devices. Accordingly, one is as likely to have an international dispute as a national one. The function of dynamic routing and facilities such as the World Wide Web, File Transfer Protocol, and remote log-on/telnet permit a user to enter, or at least to cross numerous national, state, or local borders without either the user or national authorities being aware of the user's passage. Therefore, "traditional notions of jurisdiction are outdated in a world divided not into nations, states, and provinces but networks, domains, and hosts."[40]

Trying to regulate cyberspace on a country-by-country basis is doomed to fail because it is inefficient and does not account for the inherent nature of the technology. "The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location." [41]"The unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes." Similarly, the unique nature of the cyberspace requires a uniform global system of regulation should bar nation-states from enacting inconsistent national legislation. Apart from these concerns, excessive internet censorship is one of the biggest criticisms of

[39] *ShreyaSinghal v Union of India*[2013] 12 S C C 73
[40] Anup K Ghosh, E-commerce Security and Privacy (1ST Edn. Spinger-Business Media LLC 2001) 91
[41] Communications Policy and Information Technology: Promises, Problems, Prospects, Communication Research Conference on Information, and Internet Policy (29th : 2001 : Washington D. C.)

government regulation. The Great Digital Firewall of China is one the best illustration to site on this issue.

1.4. SELF-REGULATIONS

Self-government or self-regulation is usually justified if it is: (1) more efficient; (2) the rules or adjudicatory procedures differ from the surrounding community; (3) the rules of the surrounding community are inapplicable; or (4) compliance with the rules of the community is higher, if the rules are self-enforced. Although all four factors support self-regulation, this section will focus on the first. The jurisdictional and sovereignty issue in cyberspace makes it difficult for territory-based nation-states to enforce their laws on cyberspace. Even if jurisdictional issues are solved, the infrastructure of cyberspace is evolving too rapidly for governments to regulate efficiently. The unique technical and transnational nature of cyberspace justifies self-government.

Users of the Internet rely on 'netiquette', the day to day rules for dealing with others on the Internet. They are in effect a form of customary law. The culture is widely prevalent, though the rules vary in their details. [42]If necessary they are enforced by non-legal remedies, which John Perry Barlow, the founder of the Electronic Frontier Foundation in the US, describes as ***'self-regulation'***. The technology itself allows these norms to be reinforced by users. The basic idea of self-regulation is that a community can police itself through either the development of norms of conduct, private law enforced by contract, technological architecture, or some combination of the three.

P. Trudel (1989) defines this concept as norms voluntarily developed and accepted by those who take part in an activity. Self-regulation encompasses a large number of concepts such as codes of conduct, model contracts, codes of ethics, memorandum of understanding, technical or administrative standards, certification or labelling systems. The technology itself may equally have a normative effect on behaviour and might become a source of the Internet Law when the parties are contractually referring to it or when an authority imposes it as a ***de jure (or de***

[42]Helen Robert, 'Can the Internet be Regulated?' (AUP.GOV 2011 22) <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/RP9596/96rp35>

facto)technical standard. This self-regulation, including the standard-setting process, affects fundamental public concerns and are no longer technical rules of purely commercial interest

Overall, the legislatures, regulatory agencies, and courts do not appear to be percipient in anticipating the economic and social impact of new technology. This lack of foresight suggests that these institutions should not ***unnecessarily***exercise their existing authority and not seek new authority to regulate cyberspace until either the technology and its implications become predictable or the institutions and customs of cyberspace have an opportunity to develop in response to the needs of Cyberian constituent communities and commerce. Accordingly, governments should encourage a self-regulation model.

1.5. TECHNOLOGICAL REGULATIONS

Regulators can choose whether to regulate with rules or standards. A regulator may use a standard, and thus give greater discretion to the enforcement authority, or a regulator may choose to use a rule to specify the particular outcome. Technological regulations have more in common with legal rules and do not fit neatly into the category of standards. Like rules, they regulate user behaviour, in contrast to technical standards, which merely regulate form.

In network environments, the term "standard" is largely understood to mean uniform physical and design specifications or metrics.' Like its predecessor, the legal standard, the technical standard regulates form. The infrastructure of cyberspace, for example, is defined by a unified architectural structure and standardized protocols, collectively known as the formal TCP/IP networking reference model. Technical standards do not raise serious normative issues, because they are concerned only with the form and value measurements of the Internet's infrastructure, such as quality assurances, bit size, and attached transit services.

With the evolution of standard-setting from technical to "technological" standards, that truth is no longer categorical. While technical standards regulate form, technological standards more directly regulate user behaviour. Such technological standards embed normative choices set by program designers. When technological products are standardized, firms may manipulate such standards for competitive or other advantages." Thus, technological standards, like other

delineated legal entitlements of property, may overprotect the creation and recognition of property rights in intellectual goods.

Technological designs, such as digital rights management (DRM), can be understood as a form of policymaking that may supplement or even supplant legal rules governing behaviour. Once constraints on behaviour are built into technology, the technological standards established by the constraints effectively govern the use of that technology in a manner that competes with law. Technological standards may be seen as equivalent to a licensing regime or as a form of copyright law. In some cases, technological standards can be more anticompetitive than legal rules and may give rise to antitrust concerns. From an institutional standpoint, the legal challenges created by standardized technology are present not only when firms standardize technology themselves but also when governments do so.Because technological standards act as law, they should be subjected to an optimal lawmaking analysis.

An example of a technologically designed legal command that regulates user behaviour is the standardized serial copy management system, which permits record companies to control digital copying of recorded music. In essence, it supports standardized digital equipment containing legally mandated features.

FORM REGULATION: TECHNICAL STANDARDS

When legal commands that regulate form are promoted through legal rules, they are characterized by a high level of specificity backed by an authoritative executing mechanism that leaves little room for judicial discretion. Such are many of the rules regulating civil and criminal procedural law. When commands are designed as legal standards, they are typically characterized by the level of the technical value measurements such as the quantity, weight, extent or quality they provide.

In network environments, such as cyberspace, the term "technical standards" generally means uniform physical and design specifications or metrics and, as such, technical standards are regulations of form. Formal technical standards have evolved through three categories that together define the scope of technical standards: "representational standards," "unit standards," and "similarity standards". Representational standards, the most basic class of technical

standards, define abstract quantities. Examples of representational standards are the number system, addresses, currency, and mathematical notation, such as +, -, and %. They are arbitrary human constructs without a corresponding physical representation. Unit standards define physical quantities, such as meters, miles, grams, volts, and seconds. Occasionally, these two categories of standards are combined. Human language is such a case, as it is based on specific sounds made by the human voice. In network environments, unit standards include the Open System Interconnect (OSI) reference model of the Internet's architecture, and the American Standard Code for Information Interchange (ASCII) character set, the most common standard for the 128 code numbers used by computers to represent all upper- and lowercase Latin letters, numbers, and punctuation. Lastly, similarity standards are groupings of a specific unit and representational standards that define the common physical properties of two or more entities, usually to provide some interchangeability in manufacturing, distribution, sales, and use.

In network environments, many communication standards, especially protocol standards, behave like similarity standards. ‘They define transmitting and receiving pairs, process definitions, and even quality test procedures. An example of a similarity standard in a network environment is the industry standard for information systems, the Internet ISO/IEC 15288 "Life Cycle Management-System Life Cycle Processes." **ISO/IEC** 15288 establishes a common cyclical production process of system technologies, such as the Internet, describing their technical value measurements and associated terminology.

Standards that regulate formal value measurement specifications are not unique to cyberspace. They existed in earlier information technology industries, particularly mobile telephony, high definition television (HDTV), and the radio frequency spectrum. Ultimately, the correlation between standards and form regulation was imported into the emerging governance of cyberspace. Primarily, the Department of Commerce limited the authority of the Internet Corporation for Assigned Names and Numbers (ICANN), which controls the Internet's domain name system, to "technical coordination" or routine "maintenance. In that limited regulative capacity, ICANN controls technical issues such as the maintenance of the bit size of data packets, the architecture of root services (which involves assigning Internet protocol (IP) numbers and specifying the number of top-level domains that safely be added to the root), and the preservation of unique protocol numbers for various other Internet functions. Thus, the U.S.

government authorized ICANN solely to construct technical standards aimed at regulating form but did not give ICANN any authority to regulate user behaviour. Nevertheless, this policy is not fully exhaustive or consistent, though, as both types of standards seem to be loosely merged in the 1997 Report.

SUBSTANCE REGULATION: BEHAVIORAL TECHNOLOGICAL STANDARDS

In the information age, technical standards have increasingly been incorporated into operational software designs that influence user behavior. Ultimately, the design process of these standards started to resemble the design process of software programs containing mandatory legal commands. Thus, technological standards became an aspect of software design and standard developers became closely related to programmers. To illustrate, when a specific software program is used as a testbed, the specific program in the testbed takes on the characteristics of a technological standard, implementing the information it contains. This shift is particularly evident with the development of DRM. As new markets and submarkets in network environments expand, businesses are experimenting with distribution models, such as dynamic pricing, permission to view content in exchange for user demographics, and syndication of content to other websites. One of the most controversial of these developments is DRM technology developed **by** copyright-driven industries. DRM software prevents purchasers and third parties from making unauthorized uses of digital works.**DRM** technology has two separate functions. First, it identifies digital versions of copyrighted works, just as international standard book numbers (ISBN) identify hardcopy books and stock-keeping unit (SKU) numbers identify retail merchandise." Copyright owners use two main types of existing technologies, known as "watermarking" and "fingerprinting, to create digital identifications for their works. The identification function tracks works electronically, such as when they are transmitted over basic peer-to-peer networks in the form of email or instant message attachments.

Second, DRM software may also provide copyright owners with control over the various excludable rights of copyright ownership, including access to their works and the ability to make copies of and redistribute the works. At the heart of any DRM technology is the business notion of a rights model: a scheme for stipulating to users rights to a portion of content in return for a consideration, such as registration, payment, or consent to the tracking of his or her usage.

Alternatively, many networks have architectural designs and technological standards that implement the norm of open information access.

There are two new types of technological standards specific to network environments: "compatibility standards" and "adaptive standards." Compatibility standards specify a grouping of similarity standards to support local or remote communications between independent implementations. Adaptive standards are open-ended, and allow the specification of areas left open for future revisions, manufacturer-specific options, and further study. They specify a negotiation process concerning the exchange of data between separate technological systems that includes two or more compatibility standards, and are used to establish communications.' The ability of users to access USENET, FTP, or WWW on the Internet is such a form of negotiation. Examples of adaptive standards are the IETF Internet draft 11 and the protocol extension protocol, which are designed to accommodate extensions of applications such as hypertext transfer protocol (HTTP) clients, servers and proxies. Adaptive standards allow each compatibility standard to negotiate a range of variables, including quality of communication, quantity of data transmitted, and other parameters of these systems. Thus, when protocols are open-ended by design and are used for negotiation instead of nonnegotiable incompatible transfer of user data and control, they may be considered adaptive standards. Because of the widespread use of programmable processors and the similarity to sophisticated software programs, adaptive standards are becoming increasingly important both technologically and as a mechanism to regulate user behavior.

Technological standards, which directly regulate behavior, are a different category of standards than technical standards, which only regulate form. In terms of optimal lawmaking analysis, technological standards are closely related to legal rules. For example, both substantive rules and technological standards influence user behavior directly. As technological standards' influence on behavior increases, they will increase in similarity to legal rules. Rules are best promulgated by centralized institutions, particularly public, governmental institutions. In network environments such as the Internet, however, centralized regulation is unable to keep pace with the dynamic commercialized nature of technology. Thus, the technique commonly known as technological standardization is still best kept decentralized.

1.6 NO REGULATION

The no regulation model is a null choice because, in cyberspace, the idyllic state of nature never actually existed. Cyberspace is an accidental byproduct of United States government research. Consequently, the United States government has always placed some regulation on cyberspace. For example, the NSFNET Backbone Services Acceptable Use Policy prohibits the commercial use of NSFNET. At all times the physical bodies of Cyberians could be punished for their cyberspace activities should some "real" government choose to exercise such control. Yet, governments rarely attempted to extend their jurisdiction into cyberspace. But this policy of benign neglect has changed. Governments are now interested because many individuals who are currently using the Internet can afford to invoke the judicial system to resolve disputes. The popularization of the information superhighway has educated both judges and legislatures that this is a place where real wrongs take place - wrongs that are worthy of a remedy.

1.7. LET'S SUM UP

In this chapter, we have studied the concept of cyberspace regulations. We have started with the concept of regulation of cyberspace. Then we have learnt different modules of cyberspace regulation. We have seen how these modules regulating the affairs of cyberspace. We witnessed none of the regulatory theory in isolation is completely able to regulate the cyberspace. Every theory having some pros and cons with respect to their ability in regulating cyberspace.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the necessary ingredients of regulations that address cyber laws and cyberspace?

A. The necessary ingredients of regulations that address cyber laws and cyberspace include i) legislation, ii) enforcement and iii) adjudication.

2. How has the government addressed the regulations associated with cyberspace?

A. The government addressed the regulations associated with cyberspace primarily by adapting the UNCITRAL model of e-commerce for establishing cyber laws in the country, and thereby paving the way for introduction of cyber laws in existing statutes like Information Technology Act, 2000, Indian Penal Code, 1860, Indian Evidence Act, 1872, Bankers Book of Evidence Act, etc.

3. What does cyberspace regulation aim at?

A. The aim of cyberspace regulation is to define the rules associated with use and implementation of cyberspace, to initiate appropriate actions against those who violate such regulations and adjudicating the extent of breach of such violations and imposing the required sanctions.

4. What are the positive aspects of self-regulations?

A. The positive aspects of self-regulations are that they are efficient, the rules and adjudicatory procedures differ from the surrounding community whereby the latter become inapplicable and compliance with the rules of the community is higher.

5. What is understood by DRM?

A. DRM or Digital Rights Management is a form of technological design that can be understood to be a form of policy making that may supplement or even supplant legal rules governing behavior.

1.9 FURTHER READING

- Daniel Benoliel, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 Cal. L. Rev. 1069 (2004). Available at: http://scholarship.law.berkeley.edu/californialawreview/vol92/iss4/5
- https://repository.jmls.edu/cgi/viewcontent.cgi?article=1055&context=jitpl

- Jangirala, Srinivas& Das, Ashok Kumar & Kumar, Neeraj. (2018). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems. 92. 10.1016/j.future.2018.09.063.

1.10 ACTIVITY

Elucidate the forms of regulations along with a case study that briefly explains the regulation theories of cyberspace? (1500-2000 words)

Unit 4: Cyberspace Regulatory Theory of Lawrence Lessig

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After studying this unit, the students should be able to understand:

- Define the pathetic dot theory
- Aware of different constraints pathetic dot theory viz. law, norm, market and codes.
- Interrelationship amongst these four constrains in cyberspace regulation. internet

1.2. INTRODUCTION

There are many ways to think about "regulation." Lawrence Lessig thinks about it from the perspective of someone who is regulated, or, what is different, constrained. That someone

regulated is represented by this (pathetic) dot—a creature (you or me) subject to different regulations that might have the effect of constraining the dot's behaviour. By describing the various constraints that might bear on this individual, Lessig attempted to show how these constraints function together. This idea of regulation by Lessig is known as the Pathetic Dot Theory.

Lawrence Lessig explained the regulation and the role of these four constraints with the illustration of smoking. [43]If one wants to smoke, what constraints does one face? What factors regulate the decision to smoke or not? One constraint is legal. In some places at least, laws regulate smoking—if you are under eighteen, the law says that cigarettes cannot be sold to you. If you are under twenty-six, cigarettes cannot be sold to you unless the seller checks your ID. Laws also regulate where smoking is permitted—not allowed on an airplane, or in an elevator, for instance. In these two ways at least, laws aim to direct smoking behavior. They operate as a kind of constraint on an individual who wants to smoke. But laws are not the most significant constraints on smoking. Although this illustration is not efficiently depicting the situation in India because of stringent and effective implementation of smoking laws.

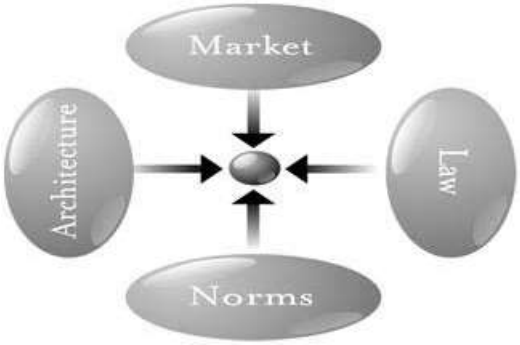
He tried to explain how by norms smoking can be regulated. Norms say that one doesn't light a cigarette in a private car without first asking permission of the other passengers. They also say, however, that one needn't ask permission to smoke at a picnic. Norms say that others can ask you to stop smoking at a restaurant, or that you never smoke during a meal. These norms affect a certain constraint, and this constraint regulates smoking behavior.

Laws and norms are still not the only forces regulating smoking behavior. The market is also a constraint. The price of cigarettes is a constraint on your ability to smoke—change the price, and you change this constraint. Likewise with quality. If the market supplies a variety of cigarettes of widely varying quality and price, your ability to select the kind of cigarette you want increases; increasing choice here reduces constraint. Finally, there are the constraints created by the technology of cigarettes, or by the technologies affecting their supply. Nicotine-treated cigarettes are addictive and therefore create a greater constraint on smoking than untreated cigarettes. Smokeless cigarettes present less of a constraint because they can be smoked in more places. Cigarettes with a strong odor present more of a constraint because they can be smoked in fewer

[43]Lawrence Lessig, Code 2.0 (Basic Books New York 3rd Edn. 2006) 54

places. How the cigarette is, how it is designed, how it is built—in a word, its architecture—affects the constraints faced by a smoker.

Thus, four constraints regulate this pathetic dot—the law, social norms, the market, and architecture—and the "regulation" of this dot is the sum of these four constraints. Changes in any one will affect the regulation of the whole. Some constraints will support others; some may undermine others. Thus, "changes in technology may usher in changes in . . . norms," and the other way around. A complete view, therefore, must consider these four modalities together.



Above said picture explained that how these four constraints can regulate any entity. In this drawing, each oval represents one kind of constraint operating on our pathetic dot in the centre. Each constraint imposes a different kind of cost on the dot for engaging in the relevant behavior—in this case, smoking. The cost from norms is different from the market cost, which is different from the cost from law and the cost from the (cancerous) architecture of cigarettes.

The constraints are different, yet they are plainly mutually supporting. Each can support or oppose others. Technologies can weaken norms and laws; they can also support them. Some constraints make others possible; others make some impossible. Constraints work together, though they function differently and the effect of each is distinct. Norms constrain through the stigma that a community imposes; markets constrain through the price that they exact; architectures constrain through the physical burdens they impose; and law constrains through the punishment it threatens.

We can call each constraint a ***"regulator"***, and we can think of each as a distinct modality of regulation. Each modality has a complex nature, and the interaction among these four is also hard to describe. I've worked through this complexity more completely in the appendix. But for

now, it is enough to see that they are linked and that, in a sense, they combine to produce the regulation to which our pathetic dot is subject in any given area. We can use the same model to describe the regulation of behavior in cyberspace.

Now we will discuss of these four constraints regulates the affairs of any entity in cyberspace.

1.3. LAW AS A MEANS OF REGULATION

Behavior in the real world — this world, the world in which I am now speaking — is regulated by four sorts of constraints. Law is just one of those four constraints. Law regulates by sanctions imposed ex-post — fail to pay your taxes, and you are likely to go to jail; steal my car, and you are also likely to go to jail. Law is prominent of regulators. But it is just one of four.

We believe in parliament's capacity to make laws to regulate the behaviour of its citizens. Where parliaments are silent, the courts will make precedents. People who break the law suffer sanctions - these can be civil penalties of loss of money when an infringing party is ordered to pay damages to another. There is also criminal law through which we believe society establishes what constitutes acceptable and unacceptable behaviour. Unacceptable behaviour is regulated through a sentencing regime – lesser offences might incur fines and bonds, more serious ones some form of a custodial sentence. We are satisfied that if parliament makes a law then it is made by the people. What is the parliament if nothing other than a delegate body of the people as articulated at elections? Once a matter becomes law the law itself ought to be a black letter – it ought to be clearly understood, free from doubt and dispute. Breaches should result in similar punishments.

Law regulates behavior in cyberspace. Copyright law, defamation law, and obscenity laws all continue to threaten ex post-sanction for the violation of legal rights. [44]How well law regulates, or how efficiently, is a different question: In some cases, it does so more efficiently, in some cases less. But whether better or not, the law continues to threaten a certain consequence if it is defied. Legislatures enact; prosecutors threaten; courts convict. We can take an illustration of Indian cyber laws that how it is regulating affairs of entities of cyberspace through framing various new legislations and by amending existing legislation.

[44]David Brake, Sharing our Lives Online: Risks and Exposure in Social Media (Palgrave Macmillan 2014) 78

Law can also regulate other constraints such as the market. The market is regulated by law not just in its elements—it is the law that enforces contracts, establishes property, and regulates currency—but also in its effects. The law uses taxes to increase the market's constraint on certain behaviors and subsidies to reduce its constraint on others. We tax cigarettes in part to reduce their consumption, but we subsidize tobacco production to increase its supply.[45] We tax alcohol to reduce its consumption. We subsidize childcare to reduce the constraint the market puts on raising children. In many such ways, the constraint of law is used to change the constraints of the market.

Law can also change the regulation of architecture. Lessig explained it as follows:

Some of the power of the French Revolution derived from the architecture of Paris The city's small and winding streets were easily barricaded, making it possible for revolutionaries to take control of the entire city with comparatively little absolute strength. Louis Napoleon III understood this, and in 1853 he took steps to change it. Paris was rebuilt, with wide boulevards and multiple passages, making it impossible for insurgents to take control of the city.

Likewise, law can regulate the architecture of cyberspace by making specific laws for intermediaries and by changing data protection mechanism.

Law can change social norms as well, though much of our constitutional jurisprudence seems dedicated to forgetting just how. Education is the most obvious example. As Thurgood Marshall put it, ***"Education is not the teaching of the three R's. Education is the teaching of the overall citizenship, to learn to live together with fellow citizens, and above all to learn to obey the law."***[46] Education is, in part at least, a process through which we indoctrinate children into certain norms of behavior—we teach them how to "say no" to sex and drugs. We try to build within them a sense of what is correct. This sense then regulates them to the law's end. Thus we have seen that how law as a separate constraint having an impact on rest of three constraints.

1.4. ROLE OF MARKET FORCE IN REGULATION

The market is the third constraint. It regulates by price. The market limits the amount that I can spend on clothes; or the amount I can make from public speeches; it says I can command less for

[45] Supra at 43

[46] Charles LZeldon, Thurgood Marshall: Race, Rights, and the Struggle for a More Perfect Union (Routledge 2013) 23

my writing than Madonna, or less from my singing than Pavarotti. Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates.
Markets regulate behavior in cyberspace. Pricing structures constrain access, and if they do not, busy signals do. (AOL learned this quite dramatically when it shifted from an hourly to a flat-rate pricing plan.) Areas of the Web are beginning to charge for access, as online services have for some time. Advertisers reward popular sites; online services drop low-population forums. [47]These behaviors are all a function of market constraints and market opportunity. They are all, in this sense, regulations of the market.[48]

We are convinced that market forces regulate behaviour. If a manufacturer creates an unsafe product this will become known to the market and consumers will not purchase these products. If a software designer wants to copyright and licence his or her work, then the market will determine if the software is worth buying as compared with that of competitors. Markets will determine what survives and what doesn't in the market place. Market forces also use price as a form of regulation. It is said consumers regulate their behavior based on a cost/benefit analysis. For example, at least theoretically, as the price of petrol rises, consumers will travel less in their cars and take public transport, or push for its installation. In its purest form, you believe that free markets, rather than the government, will best regulate human activity. In the case of cyberspace this can be understood how the accessibility of the internet very much depends on the and price charged for the accessibility of internet. It can be understood by Jio plan for accessibility of the internet and how it increases the accessibility of the internet in India.

1.5. NORMS AS REGULATORY MECHANISM

Social norms are a second. They also regulate. Social norms — understandings or expectations about how I ought to behave, enforced not through some centralized norm enforcer, but rather through the understandings and expectations of just about everyone within a particular community — direct and constrain my behavior in a far wider array of contexts than any law.[49] Norms say what clothes I will wear — a suit, not a dress; they tell you to sit quietly, and politely,

[47] Supra at 44
[48]Raymond S R Ku, Cyberspace: Cases and Materials (4thEdn. WoltersKuwer 2016) 67
[49]Richard A Spinello, Herman TTavani , Readings in Cyberethics (Jones and Barlett Publishes 2ndEdn 2004) 341

for at least 40 minutes while I speak; they organize how we will interact after this talk is over. Norms guide behavior; in this sense, they function as a second regulatory constraint. [50]

1.6 CODE OR ARCHITECTURE IN CYBERSPACE REGULATION

And finally, there is the constraint of what some might call nature, but which I want to call "architecture." This is the constraint of the world as I find it, even if this world as I find it is a world that others have made. That I cannot see through that wall is a constraint on my ability to know what is happening on the other side of the room. That there is no access-ramp to a library constrains the access of one bound to a wheelchair. These constraints, in the sense I mean here, regulate.David Hackett Fisher describes the founders of New England meticulously laying out the towns they would found so that the relationship of the buildings to each other, and to the town square, would assure that behavior within the town would be properly regulated.

In this constraint, we believe in the power of human to design systems that regulate behavior. To control speeding in a back street we would design and build speed humps. In a digital world, we believe in the power of software code to be able to create a form of regulation. For example, we might design a technological protection measure in our software that prevents a program with a license of ten users from allowing an eleventh user to open it over a network.

Bentham famously described the design of a prison so that all cells would be viewable from one central position so that prisoners would never know whether they were being watched, but that they always could be being watched, and so, they would be properly regulated.
An analogue for architecture regulates behavior in cyberspace— code. The software and hardware that make cyberspace what it constitutes a set of constraints on how you can behave. The substance of these constraints may vary, but they are experienced as conditions on your access to cyberspace. In some places (online services such as AOL, for instance) you must enter a password before you gain access; in other places, you can enter whether identified or not. In some places the transactions you engage in produce traces that link the transactions (the "mouse droppings") back to you; in other places, this link is achieved only if you want it to be. In some

[50] Ibid

places you can choose to speak a language that only the recipient can hear (through encryption); in other places encryption is not an option. [51]The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it is also regulation, just as the architectures of real-space codes are regulations.[52]

1.7. LET'S SUM UP

In this chapter, we have studied the Lawrence Lessig approach of regulation in his pathetic dot theory. We have learnt different constraints of cyberspace regulation viz. law, market, norm and code as described by Lessig in his theory. We have also understood that how these four constraints interrelated to each other and having an impact on each other's role in cyberspace. As per the approach of Lessig he considers 'code is law'. He thinks it is code which can effectively regulate the entities of cyberspace in comparison to other constrains. Although there are some serious criticism of his view but still his view still seems relevant while thinking about regulation of cyberspace. Finally, we can end the discussion of cyberspace regulation that in isolation none of the constraint can aptly regulate the entities of cyberspace, we need to consider the interrelation of each other while developing any framework for cyberspace regulation.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. How did Lessig explain the role of the constraints vis-à-vis regulation?

A. Lessig explained the role of the constraints vis-à-vis regulation through the illustration of smoking and the constraints associated therewith, for example legal. He explained that norms can regulate certain behavior thereby acting as a constraint in its exercise.

[51] William Magnuson, Blockchain Democracy: Technology, Law and the Rule of the Crowd (Cambridge University Press 2020) 567

[52]Roger Brownsword, Eloise Scotford, Karen Yeung, The Oxford Handbook of Law, Regulation and Technology (Oxford University Press 2017 1st Edn) 89

2. What are the four basic limbs of Lessig's constraint theory?

A. The four basic limbs of Lessig's constraint theory are law, social norms, market and architecture.

3. What kind of laws regulate behavior in cyberspace?

A. Behaviour in cyberspace is regulated through laws like defamation law, copyright law, obscenity laws, regulation of the market through enforcement of contracts, the establishment of property, regulation of currency etc.

4. How can market forces regulate behavior in cyberspace?

A. Market forces regulate pricing structures which in turn affect market access so as to affect consumers' approach towards certain products and hence affecting behavior in cyberspace.

1.9 FURTHER READING

- http://pne.people.si.umich.edu/kellogg/045.html
- https://harvardmagazine.com/2000/01/code-is-law-html
- https://www.kcoyle.net/lessig.html
- https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1422&context=facpubs
- Understanding Lessig: implications for European Union cyberspace policy, Taylor & Francis (2019), https://www.tandfonline.com/doi/abs/10.1080/13600860500348226?mobileUi=0&journalCode=cirl20 (last visited Nov 18, 2019).

1.10 ACTIVITY

Write an essay on the critical analysis of Lessig's theory of regulation of cyberspace. (800-1000 words)

Block 2

Fundamentals of Cyber Law

Unit 1:Outline of Legislative Framework for Cyber Law

1

SUBJECT CODE: 101

CYBERSPACE AND ITS GOVERNANCE

BLOCK 2 – FUNDAMENTALS OF CYBER LAW

UNIT 1 – OUTLINE OF LEGISLATIVE FRAMEWORK FOR CYBER LAW

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Need and Concept of cyber law
- Jurisprudence of cyber law
- Legislative framework of cyber law

1.2 INTRODUCTION

The tremendous growth and development of electronic commerce over the last decade has propelled the need for vigorous and effective regulatory mechanisms which would strengthen the legal infrastructure. All these mechanisms and infrastructures come under the purview of Cyber Law. Cyber Law has been described as that branch of law which deals with legal issues pertaining to the use of inter-networked information technology. The virtual world of internet such as computers, networks, data storage devices etc. is known as Cyberspace and the laws governing these areas are called Cyber Laws.

Cyber Law is important as it encompasses all aspects of transactions and activities on and involving the cyberspace. Cyber Law comprises of laws relating to –

- Cyber crimes
- Electronic and Digital Signatures
- Intellectual Property Rights
- Data Protection and Privacy

In India, Cyber Laws are contained in the Information Technology Act, 2000 (IT Act) which was introduced on October 17, 2000.[53] The primary purpose of the Act is to administer legal recognition to electronic commerce and to expedite filing of electronic records with the Government.

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

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

1.3 NEED FOR CYBER LAW

[53] Ajay Thakur, 'All You Need To Know About Cyber Laws In India - Ipleaders' (*iPleaders*, 2020) <https://blog.ipleaders.in/need-know-cyber-laws-india/>

Digitalization has transmuted the society as a whole. The advancement of technology and intertwined connections have paved way for a plethora of cybercrimes being committed at an unprecedented level.[54] Prior to this amelioration, the Internet was used and developed for sharing research and information in an unregulated manner. At present, it has become more transactional with enormous amount of data being transmitted via e-commerce, e-procurement, e-governance etc. Every person with a digital footprint has the power and capability to inflict considerable damage and cause calamitous harm to individuals, companies, and governments by accessing any data across the globe. Owing to such extensive development in informational technology, the word 'Privacy' has been completely taken off the books. In the light of the prodigious growth in digital population where people have become more sophisticated in the use of technology, data privacy and data protection have become the need of the hour. A robust regime has to be formulated that would deliver a careful and sensitive balance between the interests of the individual and legitimate concerns of the state.[55] All these and other varied considerations instigated a conducive atmosphere for the need for enacting pertinent cyber laws in India.

1.4 CONCEPT OF CYBER LAW

Cyberlaw is a generic term which refers to all legal and regulatory aspects of Internet and the World Wide Web.[56] Anything emanating from any legal issues concerned with any activity of citizens and others in Cyberspace comes within the ambit of Cyber Law. "Cyber" is a prefix word used to describe a person, thing or idea connected with computer, internet and information era. It has been taken from 'Kubernētēs', a Greek word for '*steersman'* or *'governor'*. The word '*Cyber'* was first used in '*Cybernetics',* coined by Mr. Norbert Wiener, which means, a study of communication and control systems in living beings and machines.[57] A vast array of information resources and services on the Internet not only provides great facilities to the society but also present opportunities for crime. The very concept of the Internet lost its essence years ago when

[54]AdemolaAdeniyi, the Need for Data Protection Law in Nigeria httpas://adeadeniyi.wordpress.com accessed on 28/10/2015

[55] Trout, B (2007) "Cyber Law: A Legal Arsenal For Online Business", New York: World Audience, Inc

[56]'CYBERLAW : PERBANDINGAN INDONESIA , SINGAPURA, DAN JEPANG' (*AndreSeptian*, 2020) <https://andreserr.wordpress.com/2015/06/10/cyberlaw-perbandingan-indonesia-singapura-dan-jepang/>

[57]Poltenson, Norman. "Mohawk Valley Is the Epicenter in the Cybersecurity Industry." The Business Journal - Central New York, vol. 30, no. 21, Central New York Business Journal, May 2016, p. S9

it got transformed for being used in several illicit and immoral activities. Several unlawful activities have been taking place acorss cyberspace, ranging from identity theft and terrorism to money laundering. Taking advantage of the anonymity offered by the internet, anybody can indulge in any sort of criminal activities with impunity. Credit card frauds, spams, defamation on the social networking sites and piracies are some of the disadvantages resulting from the illegal activities on the internet.[58] These 'grey areas' are being exploited by individuals, companies to perpetrate criminal activities in cyberspace. Cyber Law has emerged to put an embargo due to proliferation of misuse of the computer and internet in the cyberspace.

1.5 JURISPRUDENCE OF CYBER LAW

Jurisprudence has been defined as *'knowledge of law or knowledge of just and unjust'.* The two Latin words 'jus' and 'prudentia' are mutated as jurisprudence in english. Legal issues relating to digital platforms and the internet in this contemporary world have brought cyber jurisprudence into existence. Cyber Jurisprudence gives an analysis of the law regardless of territorial limitations in a space completely different from the physical world.[59] It deals with the composite idea of cyber jurisdiction and cyber court's venue in cyberspace. It provides emphasis on observing cyber uniform rules and policies at an international level. In the context of Cyberspace, Jurisprudence is manifestation of its progression and collective regulatory processes to curb all the unlawful and illicit activities through enforce laws. Cyberspace has reached an inconceivable level wherein there are no jurisdictional boundaries. For instance, an individual in India could break into the electronic vault of a bank situated in the USA using a laptop or a computer or a cellphone. Cyber Legal Jurisprudence should be an evolving process and be on the same page with the technological advancement and severity of consequential effects of

[58]'CYBERLAW : PERBANDINGAN INDONESIA , SINGAPURA, DAN JEPANG' (*AndreSeptian*, 2020) <https://andreserr.wordpress.com/2015/06/10/cyberlaw-perbandingan-indonesia-singapura-dan-jepang/>
[59]'Term Paper On Cyber Jurisprudence - Assignment Point' (*Assignment Point*, 2020) <https://www.assignmentpoint.com/science/computer/term-paper-on-cyber-jurisprudence.html.>

cybercrimes. The penalties and punishments need to have a reformative or deterrent effect on the ones committing such crimes based on the seriousness of the criminal act.[60]

In India, two legislations were passed by the Indian Judicial system to deal with cyber offences in the country i.e., The Information Technology Act, 2000 and The Information Technology (Amendment) Act, 2008. The provisions of both the laws prosecute those offences committed using computer as a medium and tool. The act penalizes various cybercrimes and provides strict punishments (imprisonment terms up to 10 years and compensation up to 1 crore rupees).

1.6 IMPORTANT TERMS RELATED TO CYBER LAW

"Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary. (Section 2(1) (b) of IT Act, 2000)[61]

"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 IT Act, 2000)[62]

"Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing electronic signature certificates. (Section 2(1) (h) of the IT Act, 2000)

"Communication Device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or images. (Section 2(1) (ha) of the IT Act, 2000)

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. (Section 2(1) (i) of the IT Act, 2000)

[60] Emerging Technologies and the Law: Forms and Analysis, by Richard Raysman, Peter Brown, Jeffrey D Neuburger and William E Bandon, III. Law Journal Press, 2002-2008 ISBN 1-58852-107-9

[61] 'Secton 2: Definitions - Information Tech. Law' (*Information Tech. Law*, 2020) <https://www.itlaw.in/secton-2-definitions/.>

[62] 'Certifying Authorities - Digital Signature Certificates' (*Digitalsignaturesale.com*, 2020) <http://www.digitalsignaturesale.com/certifying-authorities/.>

"Cyber Café" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public. (Section 2(1) (na) of the IT Act, 2000)

"Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. (Section 2(1) (nb) 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 of the IT Act, 2000 and includes digital signature. (Section 2(1) (ta) of the IT Act, 2000)

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. (Section 2(1) (w) of the IT Act, 2000)[63]

"Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary. (Section 2(1) (za) of the IT Act, 2000)

1.7 INTERDISCIPLINARY LAWS WITHIN CYBER LAW

The Government of India took effective steps for the development of information systems and the utilization of information resources after the *Information Communication Technology* revolution which commenced in 1975. Prior to that, there was no statute governing cyber laws which involved privacy, jurisdiction and issues of intellectual property rights and other legal issues. When the need arose of strict statutory laws to regulate the unlawful and illicit activities

[63]'ROLE OF INTERMEDIARIES IN THE INTERNET WORLD (Def-005) – THE CYBER LEGAL' (*Thecyberlegal.com*, 2020) <http://thecyberlegal.com/2019/09/15/role-of-intermediaries-in-the-internet-world/.>

in the cyber world and to protect the true meaning of technology, the "Information Technology Act, 2000" (ITA) heralded the new cyber law regime in the country.[64] The IT Act was passed and enacted by the Parliament of India on 17th October, 2000, comprising of 94 Sections and 2 Schedules to secure e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes.

The main objective of the Act has been to provide legal infrastructure for all the transactions carried out by means of electronic data interchange and other means of electronic communication.[65] It also aims to provide legal sanctity to all the electronic records and other activities carried out by electronic means. The Act essentially deals with the following issues:[66]

- Legal Recognition of Electronic Documents and Digital Signatures
- Offences and Contravention
- Justice Dispensation Systems for cyber crimes

The said act has also amended:

- *The Indian Penal Code, 1860*
- *The Indian Evidence Act, 1872*
- *The Bankers' Book Evidence Act, 1891*
- *The Reserve Bank of India Act, 1934*

Despite the above-mentioned amended acts, the IT Act itself specifies the acts which have been made punishable. The following statutes lay down provisions pertaining to securing digital signatures and electronic records.

- *The Information Technology (Certifying Authorities) Rules and Cyber Regulations Appellate Tribunal (Procedure) Rules* which came into force on 17th October, 2000
- *The Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules* passed on 17th March, 2003
- *The Information Technology (Security Procedure) Rules* passed on 29th October, 2003.

[64]Dhall, S C "Need a Law to Tackle CYBER CRIME" Alive, no 396, Delhi Press, Oct 2015, p 64
[65]"India : Mandate to Govern E-Commerce Industry" MENA Report, Albawaba(London) Ltd, Feb 2017
[66]'IT Act 2000 – Penalties, Offences With Case Studies - Checkmate' (*Checkmate*, 2020) <https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/.>

Some Important Provisions under The Information Technology Act, 2000[67]

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	Imprisonment up to 5 years or fine up to 10 lakh rupees.

[67]<https://www.tutorialspoint.com/information_security_cyber_law/offences_and_penalties.htm.>

	which children are shown in obscene mode	
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 in breach of lawful contract	Imprisonment up to 3 years or fine up to 5 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.

The Information Technology Act, 2000 was further amended in the form of *Information Technology (Amendment) Act, 2008* which introduced 8 new cyber offences.

1.8 INTERNATIONAL FRAMEWORK OF CYBER LAW

Cyber law has been constantly evolving ever since its inception. One of the greatest concerns in the field of cyber law is the absence of a well-defined and exhaustive framework of law across the globe.[68] There was essentially no written record of progression in this field until 1960, with the publication of the first legal article on computer law titled as, *"A Lawyer's Guide through the Computer Maze"* by Roy N. Freed. Today's Internet was built-in in the early 1960's while the initial efforts for its regulation can only be recognized in the late 1990's. The first major attempt

[68] Flanagan,anne 2005 The law and computer crime: Reading the Script of Reform. International Journal of Law and Information Technology, 13, no 1: 98-117

was taken under the auspices of the Organization for Economic Co-operation and Development (OECD), who had published a report in the year 1986, listing five categories of offences that could be considered to be constituting a common approach towards computer crime.In addition to that, The Council of European Union approved the EU Data Protection Directive on July 20, 1995 and provided guidance that they "shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data". A step to bridge the digital gap between developed and least developed countries can be traced back to 1996, publication of the United Nations Commission on International Trade Laws (UNCITRAL) Model Law and 1998, the starting of the United Nations Conference on Trade and Development (UNCTAD) global campaign to promote e-commerce especially in developing countries. The UNCITRAL was created to streamline, harmonize and unify the law of International trade. A draft of 'Model Law' was prepared after foreseeing the inadequacies and impediments that had crept in the law affecting trade. The Model Laws which have been embraced by UNCITRAL pertaining to electronic commerce and electronic signature are:

a) Model Law on Electronic Commerce 1996

b) Model Law on Electronic Signature 1998-2001

The above-mentioned model laws have played a phenomenal role in the preliminary enactment of electronic laws in various countries. WIPO Copyright Rules 1996 and WIPO Performance and Phonograms Treaty Rules 1996 govern copyright infringements and trademark issues at national and international levels. Envisaging the issues relating to cybersquatting, on October 24th, 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) approved its Uniform Domain Name Dispute Resolution Policy, for the purpose of resolving domain name disputes.

The Convention on Cybercrime,[69] also known as the Budapest Convention on Cybercrime is the first international treaty which addressed computer crime and internet crimes. The Convention and its Explanatory Report were adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8th November 2001.[70] The Convention mainly aimed at:

[69]Gordon, Sarah, and Richard Ford. 2006.On the definition and classification of cybercrime. Journal in Computer Virology, 2, no. 1: 13-20

[70] Keyser, Mike. 2003. The Council of Europe Convention on Cybercrime. Journal of Transnational Law & Policy, 12, no 2: 287-326

- Harmonizing the domestic criminal substantive law elements of offences and provisions connected in the field of cybercrime.
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences committed by means of a computer system or evidence associated with is in electronic form.
- Setting up a fast and efficient regime of international co-operation.

Different countries have had their own experiences at the time of framing and implementing cyber laws. By and large, there are many convoluted legal issues that the law enforcement agencies of different countries have witnessed from time to time and which still remain unresolved. The legislators of law on cyberspace have faced eccentric obstacles in adapting the legal principles of the traditional legal systems.

1.9 LET'S SUM UP

In this unit we have studied the need and concept of cyber space along with its jurisprudence. We have seen the important terms that needs to be noted in cyber law and the interdisciplinary laws in cyber law. Finally, we have ended our discussion with the international framework of cyber law.

1.10 FURTHER READING

- Michael D. Scott, *Scott on Information Technology Law*, Vol. 1, preface xxx, Aspen publishers, U.S.A., 3rd edn.,2007.
- R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law*, 617, Kamal Law House, Kolkata, 2009
- http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1996.tb00056.x/full.
- Compliance With Information and Communication Technology Related Multilateral Frameworks : InformationTechnology Enabling Legal Frameworks for the Greater Mekong Sub- region*, 74, Economic and SocialCommission for Asia and Pacific, United Nations Publication, 2004.*

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the various statutes associated with cyber laws in India?

A. The various statutes dealing with cyber laws in India are as follows:

- **a.** Information Technology Act, 2000
- **b.** The Indian Penal Code, 1860
- **c.** The Indian Evidence Act, 1872
- **d.** The Bankers' Book Evidence Act, 1891
- **e.** The Reserve Bank of India Act, 1934

2. What are the major areas of concern associated with and addressed by cyber laws?

A. The major areas of concern associated with and addressed by cyber laws deal with cyber crimes, electronic and digital signatures, intellectual property rights associated with cyberspace, data protection, data privacy etc.

3. Why is cyber law necessary?

A. In today's age of digitization, technology has gotten advanced to the extent wherein misuse of cyberspace can be done by one and all through various easily-accessible means and modes. Such misuse can give rise to issues of various magnitudes from violation of individual privacy and to threatened national security. Cyber laws which aim at addressing all such relevant issues are necessary for putting in place preventive measures for addressing them.

4. What are the international legal frameworks dealing with cyber laws?

A. The international legal frameworks dealing with cyber laws are EU Data Protection Directive, United Nations Commission on International Trade Laws (UNCITRAL) Model Law and 1998, United Nations Conference on Trade and Development (UNCTAD), Model Law on Electronic Commerce 1996, Model Law on Electronic Signature 1998-2001, Budapest Convention on Cybercrime.

5. What is the jurisprudence of cyber law?

A. The jurisprudence of cyber law deals with observing cyber uniform rules and policies at an international level and with curbing all the unlawful and illicit activities through enforcement of laws.

1.12 ACTIVITY

Explain the concept *'Cyber space as a metaphor'.* How would you show that the *'property in real space'* is compared with *'property in virtual space'*.Write in about 1000 -1500 words.

Unit 2: History and Emergence of Cyber Law

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Genesis of Information Technology Act
- Indian cyber law regime
- Information Technology (Amendment) Act, 2008

1.2 INTRODUCTION

In the early 1970s, countries began to adopt broad laws which were proposed to protect individual privacy. Most of the laws were based on the models introduced by the ***Organization for Economic Cooperation and Development(OECD)and the Council of Europe.***[71] The genesis

[71]Kavanagh, Camino "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" Carnegie Endowment for International Peace - Papers, Carnegie Endowment for International Peace, 28 Aug 2019

of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978). In the U.S.A., the first federal computer crime statute was the Computer Fraud and Abuse Act, 1984. The fact that only one indictment was ever made under the Act before it was amended in 1986 shows how difficult it is to write effective computer crime legislation.[72]

1.3 GENESIS OF INFORMATION TECHNOLOGY ACT

The United Nations Commission on International Trade Law (UNCITRAL)adopted the ModelLaw on Electronic Commerce in 1996 in order to bring uniformity in the law of different countries.[73] The General Assembly of the United Nations by ***Resolution No. 51/162, dated 30th January 1997*****,** recommended that all the States should give favorable considerations to this Model Law when they enact or revise their laws.

The Ministry of Commerce, Government of India created the first draft of the legislation following these guidelines termed as *"***E-Commerce Act 1998***"*. Since, later a separate ministry for Information technology came into being, the draft was taken over by the new ministry which re-drafted the legislation as ***"Information Technology Bill 1999".*** This draft was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on June 9, 2000, the act was finally notified with effect from October 17, 2000, vide notification number G.S.R 788(E).

1.4 INDIAN CYBER LAW REGIME

The Information Communication Technology revolution in India began in 1975[74] when the Government of India strategically decided to take effective steps for the development

[72]SANS Institute Information Security Reading Room
<https://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446>
[73]Meaning and Scope of information Technology Act
<https://theintactone.com/2019/05/07/bl-u4-topic-5-meaning-and-scope-of-information-technology-act/>
[74]Cyber laws regarding hacking in India – Lexlife
<https://lexlife.in/2020/03/18/cyber-laws-regarding-hacking-in-india/>

of information systems and the utilization of information resources. The National Informatics Centre under the Electronic Commission/Department of Electronics was the outcome of this view and was assisted by the United Nations Development Program (UNDP).[75] The formation of National Association of Software Services Companies in the early 1990s reflects on India's strength in this sector. Internet in India developed in 1995 and almost after 5 years, India took efficient steps to legislate its first cyber law.

The ***Information Technology Act, 2000***heralded a new cyber law regime in the country. With the advancement in changes, India became the 12th nation in the world to enact cyber laws. As outlined in the preamble of the I.T. Act, 2000, the objectives of the Act is to provide legal recognition for E-commerce transactions, facilitate Electronic Governance and to amend the Indian Penal Code, Indian Evidence Act, 1872, the Bankers' Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The Act also establishes a regulatory framework for cyber laws and lays down punishment regimes for different cyber crimes and offences.

Although the enactment of the Information Technology Act followed the UNCITRAL Model law to a considerable extent, there are, however, some areas where the I.T. Act departs from the Model Law. The deviations which were explored are quite distinct from the Model law in two key areas: digital signatures and provisions relating to online contracting. These deviations were carried out keeping in mind the legal and economic conditions prevailing in the country.

1.5 CRITICAL ANALYSIS OF THE I.T. ACT, 2000

With the enactment of the Information Technology Act, 2000, in India, law has taken a quantum jump to include even the intangibles under its purview. The Act is a proactive piece of legislation. It is to be read and understood from the point of view of *one*, facilitating international trade and *two*, as an alternative to paper-based methods of communication and storage of information. The Act is not only in tune with the UNCITRAL's Model Law on Electronic Commerce but it also unfolds various aspects of information technology to promote efficient delivery of Government services by means of reliable electronic records. The application of the

[75] An overview of cyber-crimes and cyber law in India <https://www.grin.com/document/456973>

Information Technology Act rests with the courts. It is a settled principle that the interpretation of a provision of law relates back to the date of the law itself and cannot be prospective from the date of the judgment because concededly that court does not legislate but only gives an interpretation to existing law.[76]

It was held that, a statute is an edict of the legislature. The language employed in a statute is the determinative factor of legislative intent. Words and phrases are symbols that stimulate mental references to referents.[77] The object of interpreting a statute is to ascertain the intention of the legislature enacting it.[78]

The fact is, that judiciary has always been able to assimilate technology and as the Supreme Court has observed in ***SIL Import. USA v Exim Aides Silk Importers,***[79]the need of the judiciary to interpret the statute by making allowances for any relevant technological change that has occurred. In ***Grid Corpn. of Orissa Ltd. V AES Corpn.,***[80]it was held by the Supreme Court that *"when an effective consultation can be achieved by resort to electronic media and remote conferencing, it is not necessary that the two persons required to act in consultation with each other must necessarily sit together at one place unless it is the requirement of law or of the ruling contract between the parties".*

Similarly, in ***State of Maharashtra v Dr.Praful B. Desai,*** [81] it was held that *'**videoconferencing'***is an advancement in science and technology which permits one to see, hear and talk with someone far away, with the same facility and ease as if he is present before you i.e., in your presence. In video-conferencing, both parties are in presence of each other. Thus it is clear that so long as the accused and / or his pleader are present when evidence is recorded by video-conferencing that evidence is being recorded in the ***'presence'***of the accused and would thus fully meet the requirements of Section 273 of the Criminal Procedure Code. Recording of such evidence would be as per *'procedure established by law'.* Also in ***Amitabh bagchi v***

[76]Lily Thomas v. Union of India – My Legal Partner.
<https://mylegalpartner.wordpress.com/2018/05/23/lily-thomas-v-union-of-india/>
[77]Intent: The Object of Interpretation - Blogger
<https://lawaids.blogspot.com/2010/05/intent-object-of-interpretation.html>
[78]*Institute of Chartered Accountants of India v Price Waterhouse*, AIR [1998] SC 74
[79]*SIL Import. USA v Exim Aides Silk Importers*AIR [1999] SC 1609
[80]*Grid Corpn. of Orissa Ltd. v AES Corpn* [2002] 7 SCC 736
[81]*State of Maharashtra v Dr. Praful B. Desai* AIR [2003] SC 2053

***Enabagchi,*[82]and in *BodalaMurali Krishna v Smt. BodalaPrathima,*[83]**the facility of video-conferencing was allowed.

Thus it is clear that, the Supreme Court approves of the principle of updating construction, i.e., law must constantly be on the move adapting itself to the fast-changing society and not lag behind. Moreover, the Supreme Court is advocating use of external aids to gather information. In ***Ponds India Ltd. v Commissioner of Trade Tax, Lucknow,***[84]the Court mentioned that *'Wikipedia, like all other external aid to construction, like dictionaries etc. is not an authentic source, although the same may be looked at for the purpose of gathering information'.* In ***CIT v Associated Distributers Ltd.,***[85]the Court had taken the meaning of ***'bubblegum'*** given in Wikipedia.

In the view of the fact that every second case now requires appreciation of electronic evidence on the part of the judge, it thus becomes imperative that a judge needs to wear a hat of technocrat as well! Applying technology and getting desired results is one thing, but appreciating the value of the *'evidence'* is another. One may lose evidence not because of *'lack of technology',* but because of *'lack of appreciation of technology'.* Hence, the questions before the Court of law are:

- Did the investigators / litigants take care in gathering the evidence? and
- Could they fake the evidence?

As the Supreme Court has held in ***KajalSen v State of Assam,***[86]that *'it is a duty of the court to appreciate evidence minutely, carefully, and to analyze it'.*In this context, it is interesting to note that in ***Mohammed Ajmal Mohammad Amir Kasab v State of Maharashtra,*** [87] the Supreme Court appreciated the electronic evidence, whether in the form of CCTV footage, mobile device, memory cards, data storage devices, intercepted communications over VoIP, IP Addresses, etc. while delivering the judgment.

[82]*Amitabh bagchi v Enabagchi* AIR [2005] Cal 11
[83]*BodalaMurali Krishna v Smt. BodalaPrathima* AIR [2007] AP 43
[84]*Ponds India Ltd. v Commissioner of Trade Tax, Lucknow*[2008] 8 SCC 369
[85]*CIT v Associated Distributers Ltd*[2008] 7 SCC 409
[86]*KajalSen v State of Assam*AIR [2002] SC 617
[87]*Mohammed Ajmal Mohammad Amir Kasab v State of Maharashtra* AIR [2012] SC 3565

The Information Technology, 2000 was brought to light mainly to ensure legal recognition of e-commerce in India. The provisions solely pertained to establishing digital certification processes within the country. 'Cyber Crime' as a term was taken off the books i.e., it wasn't defined in the Act. It only delved with a few instances of computer-related crimes.

Experts pointed out several flaws in the I.T Act, 2000. They were as follows:-

- The Act failed to provide any provisions regarding domain names and resolving disputes on such names.
- The Act did not explain how cyber crimes affecting computers in India committed from outside India using the Internet were to be handled.
- Many cyber crimes were not defined in the Act such as cyber defamation, cyber stalking and cyber harassment.
- The Act did not cover the privacy and protection of personal data such as medical records.
- Lastly, the Act neglected to deal with regard to Intellectual Property Rights and provide provisions to punish persons or organizations sending unsolicited emails.

It has been argued that the Act of this nature would divide society into *digital haves* and *digital have-nots.* This argument is based on the premise that with an extremely low PC penetration, poor Internet connectivity and other poor communication infrastructure facilities, a country like India would have islands of *'digital haves'* surrounded by *'digital have-notes'*. Logically speaking, such an argument is untenable as the *'digital core'* has been expanding horizontally and everyday communication connectivity is rising across India. The country is one its way to become a *'one-wired nation'.*

1.6 SUBSEQUENT DEVELOPMENTS

1.	**Information Technology (Certifying Authorities) Rules, 2000**	These rules prescribe the eligibility, appointment and working of Certifying Authorities (CAs). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended

		in 2003, 2004 and 2006.[88]
2.	**Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000**	These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.[89]
3.	**Information Technology (Certifying Authority) Regulations, 2001**	They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first was the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act and Secondly, The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.
4.	**Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002**	The IT Act was amended by the Negotiable Instruments (Amendments

[88]CH Magazine | Need for Cyber Law <https://www.chmag.in/articles/legalgyan/need-for-cyber-law/>

[89]These rules were amended in 2003 2004 and 2006 <https://www.coursehero.com/file/p4vpcvd/These-rules-were-amended-in-2003-2004-and-2006-Note-The-Act-rules-regulations/>

		and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques.[90]
5.	**Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003**	These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers. The appointment of adjudicating officers to decide the fate of multi-crorecyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws.[91]
6.	**Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004**	They prescribe provisions relating to secure digital signatures and secure electronic records.[92]

1.7 INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

[90] Introduction to Indian Cyber Law <http://www.osou.ac.in/eresources/introduction-to-indian-cyber-law.pdf>

[91] UNIT 7: Information Technology Rules Notified <https://alayalegal.com/unit-7-information-technology-rules-notified-under-the-information-technology-amendment-act-2008/>

[92] The Information Technology (Use of Electronic Records) <http://www.lexcyberia.com/pdf/The%20Information%20Technology%20(Use%20of%20Electronic%20Records%20and%20Digital%20Signatures)%20Rules,%202004.pdf>

Based on the criticism and experience gained by using the Information Technology Act, 2000, the Government set up an expert committee to review the I.T. Act in January 2005. The committee had representatives from the Government, IT Industry and legal experts and submitted its report in August, 2005. The IT (Amendment) Bill 2006, was introduced in the LokSabha on December 15, 2006, by the Union Minister of State for Communication. The 2006 Bill was modified and passed by the Parliament on 23-12-2008. It was notified after the assent of the President on 05-02-1009 as the Information Technology (Amendment) Act, 2008, (Central Act No. 10 of 2009).[93]

With the enactment of the Amended Act, the following rules came into force:-

- Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.[94]
- Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
- Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
- The Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009.
- Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity ofChairperson and Members) Rules, 2009.

1.7 CHANGES INTRODUCED BY THE AMENDED ACT

The Information Technology (Amendment) Act, 2008 is a substantial addition to India's Information Technology Act, 2000. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed

[93]UNITE INDIAN HACKERS.
<https://unitehackers.blogspot.com/>
[94]National Seminar on Enforcement of Cyberlaw, New Delhi
<https://cyberlawsconsultingcentre.com/wp-content/uploads/IT-Act-2000-vs-2008.pdf>

through it, and making corporations responsible for implementing effective data security practices and liable for breaches. The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals.[95]

There are also challenges posed by the amended Act that can be foreseen and our country needs to be well equipped to overcome these challenges. The role of Adjudicating Authority in the amended Act is very significant. The subject matter of its jurisdiction, adjudging matters alleging contravention and awarding compensation under *chapter 9* is explained in clearer terms in the Amended IT Act. The amended Act also curtails the power & jurisdiction of the Adjudicating officers and excludes those matters where compensation claimed is more than 5 crores.

The Information Technology (Amendment) Act, 2008 introduced eight new cyber offences.[96]

- Sending offensive messages through a computer or mobile phone (Section 66A)
- Receiving stolen computer resource or communication device (Section 66B)
- Punishment for identity theft (Section 66C)
- Punishment for cheating by personation using computer resource (Section 66D)
- Punishment for violating the privacy or video voyeurism (Section 66E)
- Cyber Terrorism (Section 66F)
- Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A)
- Child pornography (Section 67B)

1.8 LET'S SUM UP

In this unit we have studied the genesis of information technology act along with the critical analysis of the I.T. Act, 2000 that gives you the drawbacks in the act. We have ended our discussion with the subsequent developments and the changes that were brought in the I.T. (Amended) Act, 2008.

[95] What is Information Technology Amendment Act 2008 <https://whatis.techtarget.com/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008>

[96] Full text of "A Text book of cyber crime and penalties" <https://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt>

1.9 FURTHER READING

- http://gilc.org/privacy/survey/intro.html.
- R.K. Bagga, Kenneth Keniston (eds.), et. al., *The State, I.T. and Development*, 137, Sage Publications India Pvt. Ltd. , New Delhi, 2005.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Briefly describe the genesis of cyber laws?**

A. The basis of Cyber laws can be traced back to the laws on privacy based on the models introduced by the Organization for EconomicCooperation and Development (OECD) and the Council of Europe. However, the first laws on data protection were laid down in Germany in 1970, followed closely by the national laws in Sweden (1973), the United States(1974), Germany (1977) and France (1978) until 1984, when the USA came up with the first federal computer crime statutewas the Computer Fraud and Abuse Act. In 1996, The United Nations Commission on International Trade Law (UNCITRAL) adopted the ModelLaw on Electronic Commerce which subsequently paved the way for the Information Technology Bill, 1999 and then the Information Technology Act, 2000 in India.

2. **What are the new provisions of the Information Technology (Amendment) Act, 2008 amended following the amendment of the Information Technology Act, 2000?**

A. The provisions of the Act after amendment are as follows:

-Sending offensive messages through a computer or mobile phone (Section 66A)

-Receiving stolen computer resource or communication device (Section 66B)

-Punishment for identity theft (Section 66C)

-Punishment for cheating by personation using computer resource (Section 66D)

-Punishment for violating the privacy or video voyeurism (Section 66E)

-Cyber Terrorism (Section 66F)

-Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A)

-Child pornography (Section 67B)

3. How is the Negotiable Instruments Act related to the concept of cyber crimes?

A. The Negotiable Instruments Act deals with the concepts of electronic cheques and truncated cheques and is hence related to the concept of cyber crimes.

4. What were the drawbacks in the Information Technology Act, 2000, for which the amendment had to be introduced?

A. The drawbacks in the Information Technology Act, 2000 for which the amendment act of 2008 was introduced are as follows:

- The Act failed to provide any provisions regarding domain names and resolving disputes on such names.
- The Act did not explain how cyber crimes affecting computers in India committed from outside India using the Internet were to be handled.
- Many cyber crimes were not defined in the Act such as cyber defamation, cyber stalking and cyber harassment.
- The Act did not cover the privacy and protection of personal data such as medical records.
- Lastly, the Act neglected to deal with regard to Intellectual Property Rights and provide provisions to punish persons or organizations sending unsolicited emails.

5. Name the major rules and regulations associated with the Information Technology Act, 2000 that deal with cyber laws?

A. The major rules and regulations associated with the Information Technology Act, 2000 that deal with cyber laws are as follows:
   - Cyber Regulations Appellate Tribunal (Procedure) Rules,2000
   - Information Technology (Certifying Authority)Regulations, 2001
   - Information Technology (Qualification and Experience ofAdjudicating Officers and Manner of Holding Enquiry) Rules, 2003
   - Information Technology (Use of Electronic Records andDigital Signatures) Rules, 2004

1.11 ACTIVITY

How would you summarize the aims, objectives, salient features and critical analysis of Information Technology Act, 2000? Write in about 1000 words.

Unit 3: Outreach and Impact of Cyber Law

3

SUBJECT CODE: 101

CYBERSPACE AND ITS GOVERNANCE

BLOCK 2 – FUNDAMENTALS OF CYBER LAW

UNIT 3 – OUTREACH AND IMPACT OF CYBER LAW

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The far-reaching impacts of cyberlaw as a concept
- The ways and means of preventing cybercrimes and the active international contribution towards it

- The positive and negative impacts of cyber law and the way ahead

1.2 INTRODUCTION

In today's world, cybersecurity has become a global phenomenon affecting people across the world and creating complex social and technical challenges for governments to face. In spite of the all-pervasive presence of cyberspace and the undeniable significance of its influence across one and all, genuine awareness regarding its scope and outreach is still limited and has not sufficiently reached people at large. In spite of the large number of cyberattacks occurring every day, people tend to believe that the internet offers an invariably safe and harmless platform for use.[97] Some of the few challenges pertaining to cyber law include the ambiguities involved in the concept and the complexity linked with the social and technological aspects of cyber law. The need of the hour is to create awareness for cyber law and ensure that common people are introduced to the concept and subject-matter of cyberspace, cyber law and cybercrimes extensively. The dependence of life and various aspects thereof on cyberspace is increasing by the day. The intangibility of cyberspace, the multifaceted properties make it all the more difficult to address all the limbs of the subject matter of cyber law.[98]

1.3 OUTREACH

The growth and development of cyber law have overcome territorial boundaries and made geographic limitations irrelevant. While on one hand, it has helped foster connectivity and communications become easier and faster at a cheaper price and for better convenience, on the other, it has helped criminal activities grow on an international level. In acknowledgement of the significance of cyber law as well as its impacts, countries are not only introducing specific legislation to address the concept and its potential effects, existing frameworks of law are also being extensively amended to incorporate various facets of cyber laws.[99] As per reports, in over 90 percent instances, activities relating to cybercrime get noticed and detected only when reports

[97] Buono, L Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum* 15, 1–8 (2014) <https://doi.org/10.1007/s12027-014-0333-4>

[98] Salane, D and Misshula, E (to appear 2014) "Legislative and Regulatory Attempts to Control Cybercrime: The Good, the Bad and the Ugly"

[99] Salane, D (2013, July 31) "The Case for Strong Data Breach Notification Legislation"

are filed by victims, both individual and corporate entities and that over 80 percent instances of cybercrimes involving individual victims go unreported. Such underreporting primarily stems from lack of awareness amongst people regarding cyberspace as a whole, which in turn result in causing and creating victim shaming. It is necessary that every case of cybercrime in given specific significance and dealt with in an incident-driven approach towards every such crime committed. Likewise, law enforcement must mandatorily include both aspects of traditional techniques as well as new policies developed to incorporate modern procedural provisions. Stanford Research Institute (SRI) was first to suggest a prototype in 1973 which has by and large been followed by writers on cybercrime. The organizing schema suggested was; the computer as a subject of a crime; the computer as an object of a crime; or the computer as instrumentality. The increasing use of other devices like the cell phone or PDA required reformulation of the concept.[100] The evolving definition of cybercrime needs to accommodate the mobile phone broadband communication, wireless networks and the Internet. The definition should accommodate both current and emerging technologies.

1.4 CONCRETE GLOBAL DEVELOPMENT

Many countries across the world have enacted their own criminal laws, computer laws, information technology laws and intellectual property laws etc. to prevent and combat the cyber criminality. In view of the international dimension of cybercrime, the problem of jurisdiction arose particularly where the nationals or corporations of two or more than two countries were involved in the crime or where the criminal belongs to a different nationality and the crime was committed in a different country.[101] The crucial problem, therefore, is that the law of which country is to be applied to resolve the dispute or to try the criminal(s), particularly when there is a variation in the cyber laws and penal laws of different countries. Internet is a vast global network of computers and the feasibility of the cybercriminals to perpetrate the crime from one destination and committing the crime at other destination with anonymity urgently requires development of a universal and uniform law governing and regulating the cyberspace

[100]Brenner, Susan W and Bert-JaapKoops (2004) Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, Vol4(1), 1-46

[101]Maras, Marie-Helen (2014) *Computer Forensics: Cybercriminals, Laws and Evidence*, Second edition. Jones and Bartlett

transactions to resolve the issues of cyber criminality by mitigating the jurisdictional problem and the conflict of laws. The ever increasing phenomenon of cybercrime calls for immediate concerted efforts on the part all the countries, institutions, industries, technocrats and jurists alike to come up with universally uniform law so that the common criminals of mankind may be tried and punished without the legal and jurisdictional hassles. In this direction the international community is taking the resolute efforts to address the problem of international cyber criminality.

Global development in this direction began with the 12th Conference of the Directors of ***"Criminological Research Institutes"***of the Council of Europe, which discussed computer-related crimes for the first time in 1976. As a sequel to this conference, the Select Committee of the Council of Europe on economic Crime conducted a study of economic crime in general and made its recommendations on the same. In 1983, the ***Organization for European Co-operation and Development (OECD)***undertook a study on the harmonization of international criminal laws, which resulted into the publication of the report entitled "Computer Related Crime – Analysis of Legal Policy" in 1986.[102] The Report recommended a list of computer crimes that countries should consider prohibiting and penalizing by means of legislation:

- The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of funds or of another thing of value;
- The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery;
- The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system;
- The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put in on the market;
- The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions.

[102]Maras, Marie-Helen *Cyberlaw and Cyberliberties* Oxford University Press, forthcoming, 2020

Subsequently, the Council of Europe initiated its own study on computer crime with a view to evolving guidelines to help legislators determine the nature and nuances of computer-related crime. The Committee of Ministers, of the Council of Europe, accepted these recommendations in September 1989. The business transactions are now being carried on in the cyberspace through the nets and the online transactions have opened new vistas for unscrupulous cyber criminals to defraud and cheat the genuine businessmen and consumers. In view of the growing menace of cybercrime, the United Nations Congress in its ***13th Plenary Session*** held in 1986, adopted a resolution calling up member States to intensify their efforts to combat cybercrimes through adequate legal measures.[103]

1.5 PREVENTION OF CYBERCRIME

Preventive measures are available that help deter cybercriminals, such as passwords, firewalls, encryption, and other security policies and procedures. Cybercrime detection is a necessary last line of defence regarding loss prevention or at least loss minimization. Detection techniques include tripwires, configuration-checking tools, and anomaly detection systems. A brief overview of each of these intrusion detection techniques follows:[104]

- A tripwire is software programs that take snapshots of critical system characteristics that can be used to detect critical file changes. Tripwires provide evidence of electronic crimes since most intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics in the course of hacking the system.

- A configuration-checking tool also referred to as a ***"vulnerability assessment tool,"*** refers to software programs that detect insecure systems. Configuration-checking tools are primarily preventive in nature but used as a monitoring device they can also provide evidence regarding electronic crimes.

[103]Wall, David S (2007) *Cybercrime: The Transformation of Crime in the Information Age* Polity Press (2nd edition, forthcoming 2020)
[104]Kratchman, Stanley & Smith, Jacob & Smith, Murphy (2008) The Perpetration and Prevention of Cybercrimes

- An anomaly detection system focuses on unusual patterns of system activity. Anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in order to identify deviations from expected activity.

Cybercrime is unlikely to be identified from random and intensive searches for evidence of criminal activity.[105] If a cybercriminal can convince an intrusion detection system to continually and uselessly increase its use of computer resources, then the criminal has effectively accomplished denial of service, a particularly destructive type of cybercrime. In such a case, computer resources are wasted and cybercriminals are not detected. Since cybercrime is detrimental to business operations, business firms and their stakeholders clearly benefit from stopping cybercrime. Unless properly and continuously "fine-tuned," a single intrusion detection technique may tend to under-report cybercrimes or over-report such as excessive false alarms. In most cases, companies find it necessary to employ multiple intrusion detection techniques to efficiently and effectively detect electronic crimes.

The concept of prevention of cybercrimes[106] deals inter alia with strategies and schemes to tackle the scope and risks of occurrence of cybercrimes. To ensure sufficient measures are in place, countries implement national policies for the prevention of cybercrimes. About 40 to 50 percent countries across the world have actively recognized the necessity of establishing national policies and legislations to address cybercrimes and have acknowledged that introducing relevant legislations, developing an effective criminal justice system and spreading awareness about the concept would ensure prevention of its misuse.

With the rise in cybercrimes, research has now revealed that in most of the developing countries, individual users of internet take basic precautionary steps for securing themselves and their devices against cybercrimes. While on one hand, educating users has proved to be most effective, on the other, strengthening the societal and technological infrastructure for protection against acts of cybercrime has ensured that potential risks can be confronted. Appropriate actions must be taken by qualified professionals to successfully resolve cybercrime. Since some business

[105]Luehlfing, M, C Daily, T Phillips, and LM Smith 2003 Cyber Crimes, Intrusion Detection, and Computer Forensics Internal Auditing, 18:5 (September-October): 9-13

[106]Lakshmanan, Annamalai. (2019) Literature review on Cyber Crimes and its Prevention Mechanisms

firms may lack qualified computer security personnel, hiring outside professionals.[107] Law enforcement agencies can help with cybercrime investigations; although, many law enforcement agencies lack the technical expertise to investigate electronic crimes. Most can obtain warrants and seize computer equipment but may be unable to find the evidence needed to resolve the cybercrime.

1.6 EFFICACY OF THE EXISTING CYBER LAW

The IT Act, 2000 was amended by the IT (Amendment) Act, 2008. However, it is apposite to state that the Amendment Act could not address the legislative weaknesses of the law. This segment deals exclusively with the infirmities and shortcomings which the Amended Act is suffering from and to ascertain as to how the existing cyber law can be strengthened to make it efficacious and effective to counter the escalating menace of cybercrimes being committed against the individuals, institutions, society at writ large and the governments.[108]

While there are many legislations not only in many Western countries but also some smaller nations in the East, India has only one legislation-the I T Act, 2000. The IT Act, 2000, though a landmark legislation to deal with the cybercrime in India but the Act could not provide exhaustive measures to counter the rising trend in the cybercrime, for despite the amendment incorporated in it to attune it with the need to curb the cybercrime in view of the technological development in the area of information technology, a number of crimes and important issues have been left unaddressed. Many of the cyber crimes like cybersquatting with evil attention to extort money, Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage in the legislative scheme of the Act. In order to make the Act efficacious and effective following measures need to be addressed:[109]

[107] National Cyber Security Centre (NCSC) 2017Cyber crime: understanding the online business model p 10 <https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity>

[108] Kumar, P. N. V. (2016). Growing cybercrimes in India: A survey. Proceedings of 2016 International Conference on Data Mining and Advanced Computing, SAPIENCE 2016, 246–251 <https://doi.org/10.1109/SAPIENCE.2016.7684146>

[109]Anderson, Barton, Böhme, Clayton, Gañán, Grasso, Levi, Moore and Vasek. 2019 Measuring the Changing Cost of Cybercrime p 20 <https://weis2019.econinfosec.org/wp-content/uploads/ sites/6/2019/05/WEIS_2019_paper_25.pdf>

a) The Amendment Act of 2008 has failed to define the word —Hacking‖ or —Hacker‖, surprisingly the act of hacking with the very word —hacking‖ finds a mention in section 66 of the original Act.
b) The new amendments under Section 43-A make it mandatory for corporate-possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices.
c) The IT Rules, 2011 framed under the Sec 43-A having subsection 8(2),8(3) and 8(4) which relates to the introduction of ISO 27001 as a mandatory compliance requirement through the backdoor with the use of misleading words mentioned in the rules. ISO 27001 Compliances and Audit now has additional compliance obligation for organizations.
d) Section 79 of the amended IT Act, 2000 is not a penal section under the Act. Penalty under the Act would arise on any person or a body corporate. When an incident has occurred on account of other sections such as Sec. 43, 43-A, 65, 66, 66A, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 69, 69A, 69B, 70, 71, 72, 72A, 73, 74,84B, 84C etc. which can be brought under any of these sections and the person who is accused is otherwise an-Intermediary as defined under the Act, then the provisions of Section 79 apply. These provisions give him an opportunity to escape his liability. To use these provisions he needs to act such in a manner which can be considered as-exercising Due Diligence. The privileged intermediaries include telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.
e) The amended IT Act, 2000 has not specifically dealt with the issue pertaining to e-discovery. Today, organizations are relying increasingly upon digital evidence like email etc. and media as a means of communicating with each other and conducting business. IT Act, 2000 remains silent on this issue and also leave scope for business exploitation of e-discovery by large consulting firms at their own interpretation.
f) A Cyber Café is also a - Intermediary hence the obligations under Section 79 and the rules framed therein for - Intermediaries already apply to Cyber Cafes. The rules for Cyber Cafes are incomplete rules requiring further rules making at the State Government

level. The rules also infringe on the power of the State Government for maintaining law and order in the State.

g) Taxation of ecommerce transactions when a transaction is committed from Indian jurisdiction is not explicitly discussed nor is any passing reference made with a view to bind it with Indian tax law.

h) A clear section with regards to Jurisdiction of courts over parties staying or operating in different jurisdictions or countries is not covered. Even though having a complete separate legal jurisdiction for the cyber world, is not an expectation but certain clear guidelines necessary help lower courts and humble netizens.

i) Major offences covered under this Act are bailable. Thus interim reliefs, anticipatory bails etc. would be in a vogue with cyber criminals.

1.7 POSITIVE AND NEGATIVE IMPACTS OF CYBER LAW: THE WAY AHEAD

The gradual growth of cyber law and cyberspace over the years has brought to the fore both positive and negative aspects of the concept. It cannot be denied that owing to the vast outreach of cyber law as a concept, fighting its negatives and utilizing its positives require a multi-layered approach, which in turn demand an extensive and comprehensive understanding of the subject matter itself.[110]

While the positive impacts of cyberspace include advancement to the effect of dissolving territorial limitations, the negatives inter alia include the threat of organized cybercrime, which, arguably, acts as the biggest hazard to global banking.

Undeniably, the massive ambit of the subject itself demands that the regulations controlling it are multi-faceted. The following lists down the probable ways of controlling the effects and impacts of cyberspace.

- Ensuring that there are territorial as well as global laws to address disputes arising from use of cyberspace

[110]Presented at the International Conference: Global Perspectives on Justice, Security and Human Rights, John Jay College of Criminal Jutice, June 6-9

- The imposition of deterrent penalties to ensure the prevention of such crimes being committed
- Co-operation and inter-relationship established between various limbs of society such as firms, governments etc., for the purposes of strengthening measures of cybersecurity.

1.8 LET'S SUM UP

In this unit we have studied impacts of cyber law along with the ways and means to prevent cybercrimes and the active international contribution towards it. We have ended our discussion with the efficacy of the existing cyber law and elucidating the positive and negative impacts of cyber law.

1.9 FUTHER READING

- Donn B. Parker, S Nycum and S.S. Oura, Computer Abuse (Mento Park,, California Standford Research Institute, 1973).
- AmitaVerma, Cyber Crimes & Laws, Central Law Publication, (2009) p. 354.
- Suresh T. Vishwanathan, "The Indian Cyberlaw", at 104 (2001).

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. How do cyber laws endeavor to prevent cyber crime?

A. Basic awareness regarding cyber laws has revealed through extensive research that in most of the developing countries, individual users of internet take basic precautionary steps for securing themselves and their devices against cybercrimes. Furthermore, cyber laws have also strengthened the societal and technological infrastructure for providing protection against acts of cybercrime and ensuring ways and means of confronting risks.

2. What are the major objectives of cyber laws?

A. The major objectives of cyber laws are as follows:
   - Ensuring that there are territorial as well as global laws to address disputes arising from the use of cyberspace
   - Imposing deterrent penalties to ensure the prevention of such crimes being committed
   - Co-operating with and establishing inter-relationship between various limbs of society such as firms, governments etc., for the purposes of strengthening measures of cybersecurity

3. What are the drawbacks of cyber laws?

A. The drawback of cyber law is that it fails to keep pace with the advancement in the technology which has now dissolved territorial limitations and has threatened to initiate organized cybercrime, which, arguably, acts as the biggest hazard to global banking.

1.11 ACTIVITY

Elucidate the global developments after the I.T. Act 2000 along with the preventive measures that needs to be taken with respect to cybercrimes? (800-1000 words)

Unit 4:Major Amendments in Various Statutes

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The existing laws in the country addressing disputes and crimes related to cyberspace
- Various relevant provisions of the Information Technology Act, 2000 along with its amendment
- Various relevant provisions of the Indian Penal Code, 1860
- Various relevant provisions of the Indian Evidence Act, 1872
- Various relevant provisions of the Bankers' Books Evidence Act, 1891

1.2 THE INFORMATION AND TECHNOLOGY ACT, 2000 – RELEVANCE IN CYBER LAW

In the advanced society that we live in today, cybercrime is perceived as a phenomenon that is social and economic at the same time. Although cybercrimes are not defined in any legislation in India, nor the Information Technology Act, 2000, cybercrime is deemed to include any illegal activity that involves the internet, cyberspace or computers. The Information Technology Act along with the amendment of 2008 however address all the necessary ingredients that contribute towards the commission of cybercrime.

1.3 GENESIS OF THE I.T. LEGISLATION

The globalization of the 90's introduced a change in the economy which involved governance and growth of a society being computerized. As a result of this, international trade and commerce became dependent on electronic communication. Subsequently, the **United Nations Commission on International Trade Law (UNCITRAL)** was adopted in 1996 which acknowledged e-commerce and electronic records. To ratify and give effect to the provisions of the UNCITRAL, the Government of India enacted the Information Technology Act in 2000. Some of the unique features of the Act deal with –

- Legal recognition of electronic documents
- Legal recognition of digital signatures
- Addressing the commission of cybercrimes

The Information Technology Amendment Act, 2008 (ITAA) was passed to mark an end to all the controversies, disputes, debates and criticism arising from the nature of provisions in the IT Act. While some parts of the Act were considered draconian, others were marked as extremely dilute. The Amendment Act was hence introduced to incorporate extensive modifications into the existing Act by inter alia acknowledging the concepts of data privacy, information security, roles of intermediaries, cybercrimes like child pornography and cyber terrorism.

1.4 CONTENT

In acknowledgement of the necessity of adapting a system adept in dealing with the technological changes, the Act specifically defined the terms used in association with cyberspace, such as 'computer resource', 'communication device', 'data', 'information', 'security procedure', etc. While digital signature had been defined in the Act of 2000 as 'authentication of electronic record' using Public Key Infrastructure, the Amendment Act of 2008 gave it legal validity by re-defining it as 'digital signature and electronic signature' so as to ensure that the understanding of the term does not get dependent on the technical and technological aspects of the concepts.

The Act of 2000 further acknowledges under section 4 the validity of electronic records for recognition and maintenance of e-contracts. The Act also attempts to address data theft and misappropriation through its provisions, thereby adding a major component in the legislation. **Section 43** of the Act, the first legal provision in the country to elaborate on the civil aspects of data theft, lays down that any person accesses, downloads, copies, extracts, data from a computer or contaminates the data contained therein without the express authorization of the person owning or acting in charge of such computer shall have committed the civil offence of data theft and shall be liable to pay damages to any party affected as a result of such theft. While the Act of 2000 had capped the upper limit of such damage at Rs. 1,00,00,000/- (Rupees One Crore only), the Amendment Act of 2008 made it uncapped.

While Section 43 of the Act deals with the civil aspects of data theft, sections 65 and 66 address the criminality of such theft. Section 65 deals with computer source code being destroyed, damaged, concealed, altered or tampered with in any manner whatsoever, in contravention of the law to maintain such data. As per the Act, such offence will be punishable with imprisonment for upto three years and/or a fine of Rs. 2,00,000/- (Rupees Two Lakhs only). Section 66 addresses all acts of data theft as defined under Section 43 of the Act being with criminal intention of causing fraudulent and criminal activities and punishes such acts with imprisonment of upto three years and/or a fine of Rs. 5,00,000/- (Rupees Five Lakhs only). The Act of 2000 referred to

hacking of data within the ambit of Section 66, but the provision under the Amendment Act of 2008 eliminates such references to hacking. Additionally, a list of cognizable and non-bailable offences has been annexed to section 66 so as to widen its ambit, as listed out hereunder –

- Section 66A – addresses instances of offensive messages being sent to any device of electronic communication with the purposes of misleading or deceiving the recipient thereof regarding such message sent; whereby such instances are to be punished with imprisonment of upto three years or fine.
- Section 66B – deals with dishonest receipt of stolen computer resources or any other devices of e-communication, the punishment for which extends upto three years' imprisonment and/or a penalty of Rs. 1,00,000/- (Rupees One Lakh only).
- Section 66C – concerns with theft of identity or personal information like electronic signature and password, and imposes a punishment of upto three years' imprisonment and/or a penalty of Rs. 1,00,000/- (Rupees One Lakh only).
- Section 66D – is associated with the act of cheating by personation that involves a computer or any other device of e-communication, which shall entail a punishment of imprisonment for a term extendable upto three years and/or a penalty of Rs. 1,00,000/- (Rupees One Lakh only).
- Section 66E – deals with violation of privacy without the consent of the person concerned which shall involve entail a punishment of imprisonment for three years and/or a penalty of Rs. 2,00,000/- (Rupees Two Lakhs only)
- Section 66F – addresses cyber terrorism committed with the intention of causing unrest in the nation by threatening the security, sovereignty, unity and integrity of the country by either commission or omission of acts associated with the use and access to computer and other devices of e-communication. Acts of causing contamination in computer or e-communication devices likely to cause death/injury to people/ property shall fall within the ambits of this provision. The punishment imposed for such activities is life imprisonment.

Section 43A was introduced by the Amendment Act of 2008, to address instances wherein failure of data protection occurs owing to negligent approach towards maintenance of security

practices and thereby leads to payment of compensation. The purpose of introducing this provision was to endow upon body corporates the responsibility of protecting data and adopting reasonable security measures to that effect. The provision also imposes on the body corporate the burden to prove that sufficient security measures had been installed in the event a breach of security does indeed take place. With the same objective, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules were passed in 2011, and the Central Government simultaneously clarified the concept of 'sensitive personal data' vide a notification. Contextually, the concept of '**Cloud Computing**' becomes relevant, whereby networks of remote servers hosted on the internet instead of local servers are used to store and manage data so as to enable more organizations to deal with data belonging to other subjects stored in systems other than their own.

Section 67 as existent in the Act of 2000 was subsequently broadened by the Amendment Act of 2008 to address child pornography, and powers of intermediaries in publishing or transmitting obscene content across cyberspace in electronic format. The provision goes on to expressly capture that any individual publishing on or transmitting through cyberspace any content that is lascivious and is likely to corrupt those coming across such content, shall be imprisoned for a term of three years in prison and a fine of Rs. 5,00,000/- (Rupees Five Lakhs only) in first conviction and be imprisoned for a term of five years and/or a fine of Rs. 10,00,000 (Rupees Ten Lakhs only) in case of second conviction. In the landmark judgment of State of Tamil Nadu v SuhasKatti which was the first conviction in the country under the Information Technology Act, 2000, involved a significant role being played by section 67 of the Act. Similar to section 67, **section 67A** deals with the transmission or publishing of sexually explicit content across cyberspace and enlists it as another punishable offence. Likewise, **section 67B** addresses child pornography thereby criminalizing the act of depicting children, ie, those under the age of 18 (eighteen) years, in sexually explicit activities or creating and advertising such content, or facilitating child abuse on online platforms. The punishment under section 67B may include a fine of Rs. 10,00,000/- (Rupees Ten Lakhs only) and/or an imprisonment for upto five years. Content created or distributed for the purposes of education are however exempted under this provision. **Section 67C** endows upon all digital platforms acting as intermediaries the responsibility of maintaining necessary records as mandated by the law.

Section 69 of the Act provides to the Central Government the authority intercept, monitor or decrypt information that gets transmitted across cyberspace in accordance with the rules of compliance as established by the law and in the interest of the country. Likewise, **section 69A** allows the Central Government or its officers to block content available across cyberspace in the interest of the country; and **section 69B** deals with the power of authorizing such regulation of data through computer resource. Although it cannot be denied that this provision has the potential to be extensively intrusive, it has to be acknowledged that the Central Government has invoked the exercise of such provision only at the rarest of rare instances. The Act further releases all intermediaries of their liability in the third-party information hosted in the website of such intermediaries through **section 70**. Simply put, by virtue of this provision, intermediaries shall not be held for the content made available on/transmitted through their platforms by third parties.

The Act further provides for the establishment of quasi-judicial bodies for hearing disputes and adjudicating them by awarding compensation as well as imposing penalties for civil and criminal liabilities respectively. While Cyber Appellate Tribunal acts as the first appellate body, the High Court serves as the second one.

1.5 RELEVANCE

As opposed to the multiple legislations addressing issues of cyber law in other countries, the Information Technology Act of 2000 and the Information Technology Amendment Act of 2008 single-handedly act as the most significant law striving towards establishing a crime-free society in the country. It cannot be denied that the technology is ever growing and hence demands the law to keep pace with it and address all possible instances of cybercrimes. Although the Information Technology Act does not deal with all such probable situations, such as jurisdictional issues in cybercrimes, it covers a fairly substantial area of cyber law and acts evidently as the most significant piece of legislation on the subject.

1.6 INDIAN PENAL CODE – RELEVANCE IN CYBER LAW

The Indian Penal Code of 1860, the most significant piece of legislation on criminal jurisprudence in the country addresses the substantive facets of criminal law. In accordance with the changes in technology and the evolution and establishment of cyber laws brought in with the advent of the Information Technology Act of 2000, it became necessary to amend various sections of the Code in keeping with the new laws established. With the Act of 2000 acknowledging and recognizing electronic records and electronic evidence at the level of same importance as physical records and evidence, the ambit of the Indian Penal Code has been broadened to include electronic records and documents at par with physical records. Following such amendment, all provisions dealing with instances of false entry, or forgery of documents now include references to electronic documents and records. The provisions of the Code which have undergone amendment are as follows –

- Section 463 – Making or possessing counterfeit seal etc. with the intent to commit forgery
- Section 464 – Making a false document
- Section 468 – Forgery for the purpose of cheating
- Section 469 – Forgery for the purpose of harming reputation
- Section 470 – Forged document or electronic record
- Section 471 – Using as genuine a forged document or electronic record
- Section 474 – Having possession of forged document or electronic record knowing it to be a forgery and intending to use it as genuine
- Section 476 – counterfeiting device or marks used for authenticating documents or electronic records other than those mentioned in section 467, or possessing counterfeit marked materials.

1.7 CYBERSPACE AND THE LAW OF EVIDENCE

Electronic evidence is explicitly recognized in India and is addressed statutorily under various provisions of the Indian Evidence Act, 1872. Any electronic evidence may be produced in court though devices such as CDs, hard drives, etc. With the rise in cybercrimes, it cannot be denied that the evidence of such crimes as available in digital media gains utmost significance in the adjudication of matters relating to such crimes. Since digital evidence is invisible to common eye unless captured or stored in any specific mode or medium, thereby digitally capturing such evidence.

Section 3 of the Indian Evidence Act expressly defined that evidence shall include 'electronic records produced for the inspection of the court'. Additionally, **section 17** of the Indian Evidence Act has been amended to include that the definition of 'admission' for the purposes of the Act to include statements in electronic form as well in addition to oral and documentary admission. **Section 65A** and **65B** are to be read in sync with each other, wherein the former lays down that electronic records and their contents are to be established in accordance with section 65B, which stipulates that electronic evidence contained is to be considered admissible even in absence of the proof of the originals being produced, provided however, certain statutory technical mandates are fulfilled. The provision under section 65B is a non-obstante clause, and is hence deemed to override all general provisions on secondary evidence under the Indian Evidence Act.

1.8 THE BANKERS' BOOK EVIDENCE ACT, 1891

Similar to the provisions of the Indian Evidence Act, the Bankers' Books Evidence Act also ensures that electronic evidence produced in devices such as CD, hard drives, etc. are to be considered valid. Furthermore, the definitions clause in the Act was amended to incorporate that that any form of electromagnetic data storage device shall be included in the definition of 'bankers' books' and 'certified copy'. Additionally, a new section has been incorporated in the Act to include conditions that are to be followed while providing a printout of any certified copy, which might include data stored in digital drives or any other electronic medium.

After the enactment, as per Section 2 i.e., the definitions clause of the Bankers' Books Evidence Act was amended as: 'bankers' books include ledgers, day-books, cashbooks, account-books and

all other books used in ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device'. The amendment in the provisions of the act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms mentioned in the act.

1.9 RESERVE BANK OF INDIA ACT, 1934

The Information Technology Act, 2000 by introducing amendment in the Reserve Bank of India Act, 1934 has given it a contemporary dimension. One of the important functions of the banking system is to help the customers transfer funds to pay bills and invoices, ensure timely payment when crossing multiple time zones and fund trade transactions. It requires close coordination among the banks.[111]

In the Reserve Bank of India Act, 1934, in ***Section 58, in sub-section (2), after clause (p),*** the following clause shall be inserted, namely:-

(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in ***clause (c) of Section 45-1,*** including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund "transfers".

The insertion of aforesaid clause (pp) in the act is a step to introduce and regulate electronic fund transfer mechanism between the banks and other financial institutions. The idea is to overcome the ***'paper-trail'*** of payment transactions. The said provision calls for laying down of conditions for interbank participation in fund transfers, manner of such fund transfers and the rights and obligations of the participants in such transfers.

1.10 LET'S SUM UP

[111] AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934 <http://www.cyberlawclinic.org/rbi.htm>

In this unit we have studied the existing laws in the country addressing the disputes and the crimes pertaining to cyberspace. We have seen the relevant provisions along with the various amendments that took place in Indian Penal Code, Indian Evidence Act, The Bankers' book Evidence Act and finally The Reserve Bank of India Act.

1.11 FURTHER READING

- Iibf.org.in (2019), http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf (last visited Nov 16, 2019).
- http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160
- Acadpubl.eu (2019), https://acadpubl.eu/hub/2018-119-17/2/141.pdf (last visited Nov 16, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the existing laws in the country addressing disputes and crimes related to cyberspace?**

A. The existing laws in the country addressing disputes and crimes related to cyberspace are as follows:

- Information Technology Act in 2000
- Information Technology Amendment Act, 2008
- Provisions in various other existing legislations that were amended owing to the introduction of the Acts of 2000 and 2008.

2. What are the relevant provisions of the Information Technology Act associated with cyberspace?

A. The relevant provisions of the Information Technology Act associated with cyberspace are as follows-

- Section 66 – Computer related offences (including the sub sections to section 66)

- Section 67 – Punishment for publishing or transmitting obscene materials in electronic form (including the sub sections to section 67)

- Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

- Section 70 – Protected System

- Section 43 – Penalty and compensation for damage to computer, computer system etc.

3. What are the relevant provisions of the Indian Penal Code, 1860 associated with cyberspace?

A. The relevant provisions of the Indian Penal Code, 1860 associated with cyberspace are as follows:

- Section 463 – Making or possessing counterfeit seal etc. with the intent to commit forgery

- Section 464 – Making a false document

- Section 468 – Forgery for the purpose of cheating

- Section 469 – Forgery for the purpose of harming reputation

- Section 470 – Forged document or electronic record

- Section 471 – Using as genuine a forged document or electronic record

- Section 474 – Having possession of forged document or electronic record knowing it to be a forgery and intending to use it as genuine

- Section 476 – counterfeiting device or marks used for authenticating documents or electronic records other than those mentioned in section 467, or possessing counterfeit marked materials

4. What are the relevant provisions of the Indian Evidence Act associated with cyberspace?

A. The relevant provisions of the Indian Evidence Act associated with cyberspace are section 3, section 17, section 65A and section 65B.

1.13 ACTIVITY

Explain in detail admissibility of electronic evidence with the help of case laws. (1000 words)

Block 3
Personal Jurisdiction in Cyberspace

Unit 1: Establishment of Personal Jurisdiction in Cyberspace

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The U.S. Approach to Personal Jurisdiction
- Nature of websites
- Interactive and Passive Websites

1.2 INTRODUCTION

E-Commerce is 24/7 commerce. It is an online activity involving the exchange of goods and services for a consideration (money). Such activity may lead to disputes, which could be (a)

municipal (domestic) or (b) international. The question is how to resolve these disputes keeping in view the complexity of the online activity.

The resolution depends on identifying the 3Ws of the online dispute: What, Where and Why. From the point of identifying the jurisdiction, it is important to know the nature of the dispute and for that purpose, the following questions are necessary:

- What has happened?
- Where did it happen? and
- Why did it happen?

The answers would provide not only the necessary information related to the business model of the website but also the extent of commercial interaction between the service provider (website owner) and the user.

The traditional principles of domestic and international jurisdiction that have been developed and adopted over a period of time are now being extended to cyberspace to formulate a new idiom of cyber jurisdiction. This adoption, in a way, would maintain continuity of established law and practice even in the realm of online activities.

1.3 THE U.S. APPROACH TO PERSONAL JURISDICTION

It is important to understand the enactments of the long-arm statute and the due process of law of the U.S. Constitution to know how these principles have been used by various courts to resolve e-commerce related disputes.

The principle ***'long-arm statute'*** authorizes the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the state on the ground that their action (tortious or any other) falls within the nature of activity required to qualify for jurisdiction.

Over a period of time the States of the US have developed their own respective long-arm statute to exercise personal jurisdiction over any non-domiciliary *"who commits a tortious act within the state"* as long as the cause of asserted arises from the tortious act.

The ***'due process of law'*** as given in the fifth and fourteenth amendment of the US constitution limits the powers of the courts to exercise traditional notions of fair play and substantial justice. The Fourteenth Amendment to the US Constitution provides that *"no state shall deprive any person of life, liberty or property without due process of law".* The idea is to invoke both long-

arm statute and due process of law provisions to allow the court to exercise personal jurisdiction over any non-domiciliary defendant.[112]

Motion to Dismiss for lack of personal jurisdiction over a non-resident defendant.

End User (Plaintiff)	E-Business (Defendant)
To prove:	
The local state "long-arm statute" applies	Defendant to file and argue a motion to dismiss for lack of personal jurisdiction
There is no violation of defendant's due process rights under the Constitution provision(s).	

1.4 ESTABLISHING PERSONAL JURISDICTION

The credit to establish ground rules for establishing personal jurisdiction for the non-resident lies with the US Supreme Court judgment in ***International Shoe Co. vs State of Washington, Office of Unemployment Compensation and Placement et al***[113]**.** It held that a court's exercise of personal jurisdiction over a non-resident defendant is proper if that defendant has had certain minimum contacts with (the forum state) such that the maintenance of the suit does not offend *'traditional notions of fair play and substantial justice'.*[114]It established three criteria for establishing ***"minimum contacts":***

- The defendant must *"purposeful avail"* himself of the privilege of doing business with the forum state.
- The cause of action arises from the defendant's activities in the forum state, and
- The exercise of jurisdiction would be fair and reasonable.

The *'minimum contact'* principle laid the foundation of the state's jurisdiction over other state's subject. It advocated the establishment of minimum contacts to give rise to obligations between

[112]Bensusan Restaurant Corp v King - H2O Classroom Tools <https://h2o.law.harvard.edu/cases/4341>

[113]*International Shoe Co. vs State of Washington, Office of Unemployment Compensation and Placement et al* 326 US 310 [316] [1945]

[114]Sykes, Phillip, and Laura McCarthy "Are You Defending Your Clients Where They Don't Belong? Corporate Defendants' New Potent Defense Is Personal (Jurisdiction, That Is)" Defense Counsel Journal, vol 82, no 3, International Association of Defense Counsel, July 2015, p 282

the defendant and the forum state. Primarily, it does not look into the issue whether the contacts were sufficient or insufficient to establish *'purposeful availment'.*

The ***International Shoe Company case*** was decided in the year 1945, and at that time, there were no state long-arm statutes. The long-arm statute went a step ahead of minimum contacts to look into whether the contacts were sufficient to establish purposeful availment like

- Purposefully and successfully solicitation of business from forum (state) residents.
- Establishment of the contract with the forum (state) residents.
- Associated with other forum (state) related activity
- Substantial enough connection with the forum (state)

Once the court determined that sufficient minimum contacts existed to exercise specific jurisdiction over the defendant, the court then would have to consider whether it was reasonable to subject the non-resident defendant to the personal jurisdiction of the forum to the extent that federal constitutional requirements of due process will allow.

The importance of the *International Shoe Company case* is that it established for the first time that personal jurisdiction might exist even though the defendant had no physical presence in the forum state. It acted as a precursor to the states' long-arm statutes. Later, with the advent of e-commerce, this judgment has been used by the courts all over the United States as an established law in identifying minimum contacts to claim personal jurisdiction over a non-resident.

In a nutshell, a state court may acquire valid, specific personal jurisdiction over a non-resident defendant only if:

a) The state's long-arm statute provides for jurisdiction under the factual circumstances and
b) The defendant has had sufficient minimum contacts with the state such that the exercise of jurisdiction does not offend *'traditional notions of fair play and substantial justice',* violating the due process clause of the 14th amendment.[115]

1.5 ESTABLISHING PERSONAL JURISDICTION IN CYBERSPACE

[115] *KAHN v MAICO COMPANY* 216 F.2d 233 [1954] <https://www.leagle.com/decision/1954449216f2d2331376>

The courts have been borrowing the principles of personal jurisdiction and extending them to the cyberspace setting. The principles of jurisdiction, which were earlier applied to physical establishments, are now being successfully applied to online business establishments (websites).
A website represents a virtual business model. In order to fix the place of jurisdiction, one may have to look into the nature of the websites model – whether it is ***'business-oriented'*** or ***'information-oriented'.*** Other key elements that have to be taken into consideration are: geographical location of users, websites owner and the web server. Even the terms of service agreements, disclaimers and choice of law or forum clauses play an important role.

1.6 NATURE OF THE WEBSITE

An online form of business may exist either in the form of ***(a) Passive website or (b) Interactive website.*** As the name suggest, *'passive'* website is meant for information purposes only, whereas an *'interactive'* website is a dynamic website and provides more than mere information.

Passive Website	Interactive Website
Provides only information	Provides information and facilitates purchasing decisions
Does not solicit business	Purposefully solicits business
Not a revenue model per se	Represents a revenue model
Personal Jurisdiction does not exist	Personal Jurisdiction may or may not exist depending upon fulfillment of the minimum contacts test

Application of minimum contacts and the long arm of statute principles have been used by the courts to determine personal jurisdiction by differentiating between *passive* and *interactive* websites. An important element of minimum contacts is that the contacts need to be of such a character and degree that a defendant could reasonable have expected to be hauled into court in the distant state.

1.7 INTERACTIVE WEBSITES

In ***Cody vs Ward***[116]**,** a Connecticut resident brought suit in Connecticut against a California resident, claiming reliance on fraudulent representatives made by the defendant resulting in a loss.

The court held that it had valid jurisdiction over the defendant based solely upon bulletin board messages posted by the defendant on an online service's ***"Money Talk"*** bulletin board and e-mail messages and telephone conversations from the defendant in California to the plaintiff in Connecticut. It simply concluded that the ***purposeful availment***requirement was satisfied by the defendant's electronic contacts with the plaintiff.

Further in ***CompuServe, Inc. vs Patterson***[117]**,** CompuServe, an Ohio corporation with its main offices and facilities in Ohio, sued one of its commercial shareware providers, a resident of Texas. The suit was filed in Ohio, and the defendant asserted that the Federal District Court in Ohio lacked jurisdiction over him, claiming never to have set foot in Ohio.

The appellate court measured the defendant's ***'contacts'*** with Ohio and concluded that jurisdiction was proper because: **(a)** the defendant has purposefully availed himself of the privilege of doing business in Ohio by subscribing to CompuServe and subsequently accepting online CompuServe's Shareware Registration Agreement (which contained an Ohio choice of law provision) in connection with his sale of shareware programs in the service, as well as by repeatedly uploading shareware programs to CompuServe's computers and using CompuServe's e-mail system to correspond with CompuServe regarding the subject matter of the lawsuit; **(b)** the cause of action arose from Patterson's ***'activities'*** in Ohio because he only marketed his shareware through CompuServe; and **(c)** it was not unreasonable to require Patterson to defend himself in Ohio because by purposefully employing CompuServe to market his products, and accepting online the Shareware Registration Agreement, he should have reasonable expected disputes with CompuServe to yield lawsuits in Ohio.

Similarly, in ***EDIAS Software International vs BASIS International, Ltd.,***[118]where an Arizona based software distributor brought suit in Arizona against a New Mexico software development company arising out of the termination of an agreement between the companies and public statements made by the defendant about the termination. The defendant had no offices in Arizona.

---

[116]*Cody v Ward* 954 F Supp 43 D Conn [1997]

[117]*CompuServe, Inc v Patterson* 89 F 3d 1257 6th Cir [1996]

[118]*EDIAS Software International vs BASIS International, Ltd* 947 F Supp 413 [1996]

The defendant's contacts with Arizona analyzed under the purposeful availment test consisted of: **(a)** a contract with the plaintiff (executed in New Mexico with a New Mexico choice of law provision); **(b)** phone, fax and e-mail communications with plaintiff in Arizona; and **(c)** sales of software products to the plaintiff and other Arizona residents; and visits to Arizona by officers of the defendant. The court upheld the plaintiff's claim of personal jurisdiction over the defendant.
If one analyses the aforesaid three cases, then one may conclude that all the three cases fall in the category of an interactive website, though their degree of interactivity differ:

Minimum **Level of Personal Interactivity** **Maximum**

Cody vs Ward < CompuServe, Incvs Patterson < EDIAS Software International vs BASIS International, Ltd.

In ***Cody vs Ward,*** the level of personal interactivity has been limited to posting of bulletin board messaged and telephonic conversation from the defendant based in California to the plaintiff based in Connecticut, where in ***CompuServe, Inc. vs Patterson,*** the relationship though online, was of a commercial nature. In ***EDIAS Software International vs BASIS International, LTD.,*** the online interaction has been further supported by offline activities, like sale of the goods and visits to Arizona by officers of the defendant.

1.8 INTERACTIVE 'MIXED' WEBSITES

Now supposing that if a company maintains a website for the purpose of soliciting business, then would it be called an interactive website. In ***Maritz, Inc. vsCybergold, Inc.***[119]the court looked at the very basic issue of maintaining a website by the company by framing the due process issue as whether ***"maintaining a website which can be accessed by any internet user, and which appears to be maintained for the purpose of, and in anticipation of being accessed and used by any and all internet users, including those residing in Missouri (accessed 131 times by residents of the forum state), amounts to promotional activities or active solicitations such as***

[119]*Maritz, Inc. vCybergold, Inc*947 F Supp 1328 E D Mo [1996]

to provide the minimum contacts necessary for exercising personal jurisdiction over a non-resident".[120]

The court concluded that because the maintenance of a website is a more efficient and faster means of reaching a global audience, and through its website, CyberGold has consciously decided to transmit advertising information to all internet users, knowing that such information will be transmitted globally. Thus, CyberGold's contacts are of such quality and nature, albeit a very new quality and nature for personal jurisdiction jurisprudence, that they favor the exercise of personal jurisdiction over the defendant.

The court reasoned that setting up a website is a stronger basis for jurisdiction than maintaining a telephone number or a mailing address, since **(i)** a company's establishment of a telephone number, such as an 800 number, is not as efficient, quick, or easy way to reach the global audience that the internet has the capability of reaching, and **(ii)** if a forum resident sends a letter to defendant, (defendant) would have the option as to whether to mail information to the (forum) resident, (whereas defendant) automatically and indiscriminately responds to each and every internet user who accesses its website.

In other words, specially maintaining a website for soliciting business i.e., advertising and promoting the offline activities in an online medium, exemplifies the fact that the website is an interactive one, though of a lesser degree.

Does this mean that maintaining a website for information purpose only would fall in the interactive category?

1.9 PASSIVE WEBSITES

In ***Bensusan Restaurant Corp. vs King,***[121] where a New York jazz club operator sued a Missouri club owner claiming trademark infringement, dilution and unfair competition over the use of the name ***"The Blue Note".*** The defendant maintained a website promoting his Missouri *Blue Note* club and providing a Missouri telephone number through which tickets to the club could be purchased.[122]

[120] *Maritz, Inc v Cybergold, Inc,* 947 F Supp. 1328 <https://law.justia.com/cases/federal/district-courts/FSupp/947/1328/1453704/>

[121] *Bensusan Restaurant Corp v King* 937 F Supp 295 SDNY, [1996]

[122] Cyber Law Cases &Judgements - Advocate Prashant Mali

The issue, as framed by the Federal District Court, was whether the existence of the website, without more, was sufficient to vest the court with personal jurisdiction over the defendant under New York's long-arm statute.

The Court held that it did not. The court considered whether the existence of the website and telephone ordering information constituted an ***offer to sell*** the allegedly infringing product in New York, and concluded it was not. The court noted that, although the website is available to any New Yorker with Internet access, it takes several affirmative steps to obtain access to this particular site, to utilize the information contained there, and to obtain a ticket to the defendant's club.

These steps would include the need to place a telephone call to Missouri and to physically travel to Missouri to pick up the tickets ordered. Therefore, the court concluded that any infringement that might occur would be in Missouri, not New York. The mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York.

It found that the defendant did nothing to purposefully avail himself of the benefits of New York. There was no evidence of the defendant actively encouraging New Yorkers to visit the site.

The nature of a website – whether interactive, mixed or passive depends on the business model the said website is subscribing. It is the degree of interactivity that separates an interactive website from the passive one. The level of interactivity has to take into consideration the purposeful availment of the benefits of the forum state in the form of conducting business online and/or offline.

1.10 LET'S SUM UP

In this chapter, we have studied the U.S. Approach to personal jurisdiction along with the jurisdiction in cyberspace. We also studied the nature of the website and finally, we ended the discussion with the interactive websites and passive websites.

1.11 FURTHER READING

<http://www.prashantmali.com/cyber-law-cases>

- Cyber law – Text and Cases, (Ferrera, G.R., Lichtenstein, D.S., Reder, M.E.K., August, R., Schiano, W.T.), West Thomson Learning, USA, 2000, p.21.
- See Jean Gleason & Robert Rosenblum, Current Developments in Regulation D and Rule 144A: The SEC's Efforts to Increase the Effectiveness and Liquidity of the U.S. Private Placement Market, C540 ALI-ABA 443, 449 (1990).
- Jiménez, William and Lodder, Arno R., Analyzing Approaches to Internet Jurisdiction Based on Model of Harbors and the High Seas (August 13, 2015). International Review of Law, Computers & Technology, Vol. 29, No. 2/3, July 2015, p. 266-282.
- See generally Joseph Kalo, Jurisdiction as an Evolutionary Process: The Development of Quasi In Rem and In Personam Principles, 1978 DUKE L. J. 1147 (tracing relationship between jurisdictional evolution and economic development).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the long-arm statute?

The principle ***'long-arm statute'*** authorizes the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the state on the ground that their action (tortious or any other) falls within the nature of activity required to qualify for jurisdiction.

2) What is due process of law?

The ***'due process of law'*** as given in the fifth and fourteenth amendment of the US constitution limits the powers of the courts to exercise traditional notions of fair play and substantial justice. The Fourteenth Amendment to the US Constitution provides that *"no state shall deprive any person of life, liberty or property without due process of law".* The idea is to invoke both long-arm statute and due process of law provisions to allow the court to exercise personal jurisdiction over any non-domiciliary defendant.

3) Differentiate between Passive and Interactive Website?

Passive Website	Interactive Website
Provides only information	Provides information and facilitates purchasing decisions

Does not solicit business	Purposefully solicits business
Not a revenue model per se	Represents a revenue model
Personal Jurisdiction does not exist	Personal Jurisdiction may or may not exist depending upon fulfillment of the minimum contacts test

1.13 ACTIVITY

Explain the personal jurisdiction in cyberspace along with different types of websites and case laws pertaining to it? (1000 words)

Unit 2: Overview of Tests and Interactivity

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Sliding Scale Approach
- Forum State Targeting
- The Effects test

1.2 SLIDING SCALE APPROACH

In ***Zippo Manufacturing Company vs Zippo Dot Com, Inc.,***[123] Zippo Manufacturing Company, a Pennsylvania based corporation has been well known among other things for ***'Zippo'*** tobacco lighters. Zippo Dot Com, Inc. California corporation has been providing free news services

[123] *Zippo Manufacturing Company v Zippo Dot Com, Inc*952 F Supp 1119 W D Pa[1997]

through its website. In addition, the defendant also provided a fee-based service to permit the subscriber to view and/or download Internet newsgroup messages that are stored on the defendant's server in California. The defendant, a California corporation, was sued in Pennsylvania.

Dot Com maintained no offices, employees or agents in the state of Pennsylvania. It has been posting information about its service on its web pages, which are accessible to Pennsylvania residents via the Internet. The defendant had 140,000 paying customers worldwide and out of which around 2%, i.e., 3,000 were Pennsylvania residents. In addition, it had contracted with several Internet access providers in Pennsylvania to permit the Pennsylvania subscribers to access the Dot Com's new service.

Court task was to determine whether Dot Com's conducting of e-commerce with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania. Dot Com not only chose to process Pennsylvania residents' applications but also assigned them passwords.

The Dot Com argued that its forum-related activities were not numerous or significant enough to create a ***'substantial connection'*** with Pennsylvania. It pointed out to the fact that only 2% of its subscribers were Pennsylvania residents.

The court concluded that this level of contact with the state justified the exercise of specific personal jurisdiction. In doing so, however, it reviewed the growing number of cases in the *genre* and tried to provide some synthesis of the varying approaches. The court noted that the cases reveal a ***'sliding scale',*** in which, At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. (***e.g. Compuservevs Patterson)***. At the opposite end are situations where a defendant has simply posted information on an Internet Website, which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction ***(e.g. Bensusan Restaurant Corp., vs King).*** The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and (the)

commercial nature of the exchange of information that occurs on the website. ***(e.g. Maritz, Inc. vsCybergold, Inc.).***

Nature of website	Personal Jurisdiction
Interactive	(+)
Mixed	(+) or (-)
Passive	(-)

To sum up, the sliding scale approach classifies the websites on the basis of interactivity. In ***Bensusan,*** the court refused to exercise jurisdiction based on the website alone, reasoning that it did not rise to the level of purposeful availment of that jurisdiction's laws whereas in ***CompuServe*** the user had *'reached out'* from Texas to Ohio and originated and maintained contacts with Ohio.

These judgments have underlined the fact that personal jurisdiction must adapt to progress in technology and that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportional to the nature and quality of commercial activity that a business entity conducts over the Internet.

1.3 THE LIMIT OF INTERACTIVITY CRITERION

Over a period of time (especially post 1997), the courts have moved away in some cases from the sliding-scale prognosis that personal jurisdiction is directly proportional to the nature and quality of commercial activity that a business entity conducts over the Internet. For example, in ***CyberSell Inc. vsCyberSell Inc.***[124] the court endorsed the sliding-scale set forth in ***Zippo,*** held that mere operation of a website is insufficient to support personal jurisdiction: something more is required to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial wat to the forum state. It concluded, on the facts of this case, that something else was lacking and declined personal jurisdiction over the defendant.

[124] *CyberSellInc vCyberSellInc*130 F 3d [414] 9th Cir [1997]

Similarly, the courts from the other states have not been willing to accept that interactivity of a website alone constitutes ***'purposeful availment'*** of the forum state. Cases in which interactive features of a website were found insufficient to support jurisdiction include: ***3D Systems, Inc. vsAarotech Laboratories, Inc.,***[125] (defendant operated a website describing its subsidiary's products, and received e-mail inquiries via that site, but merely forwarded them to its subsidiary for response); ***American Information Corp. vs American Infometrics, Inc.,***[126] (prospective employees could submit their resumes via the website); ***Ecotecture, inc.vsWenz,***[127] (website allowed visitors to subscribe to an online journal); ***People Solutions, Inc. vs People Solutions, Inc.,***[128] (website contains interactive pages that allow customers to test Defendant's products, download product demos, obtain product brochures and information, and order products online); ***JB Oxford Holdings Inc. vs Net Trade, Inc.,***[129] (visitors could apply for a securities trading account online); ***Desktop Technologies Inc. vsColorworks Reproduction & Design, Inc.,***[130] (site allowed exchange of files via FTP and e-mail); ***Agar Corp. vs Multi-Fluid, Inc.,***[131] (site included links allowing visitors to provide feedback and register).

It seems that the courts have started appreciating and analyzing the website in a holistic fashion rather than in a piecemeal manner. To them, interactivity is not the only criteria for proclaiming personal jurisdiction. Similarly, the features on the website, like a toll-free number and/or link to send an email do not make such website interactive. For example, in ***Osteotech, Inc. vsGenSci Regeneration Sciences, Inc.,***[132] (placement of defendant's phone number or e-mail address on its website is not relevant to the jurisdictional analysis since inclusion of this information has no more of an impact on any particular forum than a website without such information); ***Edberg vsNeogen Corp.,***[133] (no jurisdiction, where site included both a toll-free number and a link for sending e-mail to the defendant); ***Grutkowskivs Steamboat Lake Guides & Outfitters, Inc.,***[134] (inclusion of an e-mail link and local telephone number does not make site interactive); ***Conseco,***

[125] *Systems, Inc vAarotech Laboratories, Inc*160 F 3d 1373 Fed Cir[1998]
[126] *American Information Corp v American Infometrics, Inc*139 F Supp 2d 3696 D Md[2001]
[127] *Ecotecture, inc vWenz*[2000] WL 760961
[128] *People Solutions, IncvPeople Solutions, Inc*[2000] WL 1030619 N DTex [2000]
[129] *JB Oxford Holdings Inc v Net Trade, Inc* 76 FSupp 2d 1363 S D Fla [1999]
[130] *Desktop Technologies Inc vColorworks Reproduction & Design, Inc*[1999] WL 98572 E D Pa[1999]
[131] *Agar Corp v Multi-Fluid, Inc*45 U S P Q 2d BNA 1444 S DTex [1997]
[132] *Osteotech, Inc vGenSci Regeneration Sciences, Inc*6 F Supp 2d 349 D N J [1998]
[133] *Edberg vNeogen Corp* 17 F Supp 2d 104 D Conn [1998]
[134] *Grutkowski v Steamboat Lake Guides & Outfitters, Inc*[1998] WL 962042 E D Pa [1998]

Inc. vsHickerson,[135] (no jurisdiction, where site included e-mail link); ***Transcraft Corp. vsDoonam Trailer Corp.,***[136] (no jurisdiction, where site includes a toll-free number and invites inquires by e-mail).

1.4 INTERACTIVITY: ONLINE + OFFLINE

As discussed previously, on the scale of interactivity, the 'plaintiff-defendant' interaction in ***EDIAS Software International vs BASIS International, Ltd.,***[137]has been identified as the highest (maximum) since the online interaction between them has been further supported by offline activities, like sale of the goods and visits to Arizona by officers of the defendant.

Increasingly, courts have been going beyond the online interaction and looking at whether there has been some ***'additional contacts'*** to satisfy due process requirements for jurisdiction. For example, in ***Starmedia Network, Inc. vsStarMedia Ins.,***[138]the defendant's website allowed visitors to register, download dealer applications, obtain password-protected product and pricing information. The criteria, but found that its interactivity was limited. It held, however, that the due process requirements for jurisdiction were satisfied in view of additional contacts that defendant had with the forum state. Similarly, in ***Hsin Ten Enterprise USA, Inc. vs Clark Enterprises,***[139] the court did not ground jurisdiction on defendant's interactive website alone, but noted that defendant sent representatives to attend trade shows in the forum state, maintained independent affiliates there, and had sold its products to residents of the forum state.

Hence, it is important to note that the meaning of website interactivity does no longer imply online interaction only. The courts have been looking into some additional offline contacts for proper application of personal jurisdiction.

1.5 FORUM STATE TARGETING

Another trend that has been emerging is that the courts are now increasingly taking cognizance of the commercial involvement of the residents of the forum state. The earlier concept of

[135] *Conseco, Inc vHickerson*698 N.E.2d 816 Ind App [1998]
[136] *Transcraft Corp vDoonam Trailer Corp*45 U S P Q 2d (BNA) 1097 N D Ill [1997]
[137] *EDIAS Software International v BASIS International, Ltd*947 F Supp 413 D Ariz[1996]
[138] *Starmedia Network, Inc vStarMedia Ins*[2001] WL 417118 (SDNY 2001)
[139] *Hsin Ten Enterprise USA, Inc v Clark Enterprises*138 FSupp 2d 449 SDNY [2000]

'general interaction' has given way to ***'specific interaction'*** for the purpose of invoking special personal jurisdiction. For example, In ***Millennium Enterprises Inc. vs Millennium Music, LP,***[140] the plaintiff which operated music stores in Oregon under the name *'Music Millennium,'* claimed that defendant violated its trademark in that name by operating in South Carolina under the name *'Millennium Music'*. Defendant's website allowed visitors to purchase compact disks, join a discount club, and request franchising information, but no residents of Oregon had made any purchases via the website or engaged in any online communication with the defendant. The court rejected the view that potential interactivity is sufficient to satisfy due process. It held that there must, in addition, be some *'deliberate action'* with the forum state, consisting of either transactions with residents of the forum state or other conduct purposefully directed at them. The court opined, 'Until transactions with Oregon residents are consummated through defendants' Website, defendants cannot reasonably anticipate that they will be brought before this court'.

Also, in ***Quokka Sports, Inc. vs Cup Int'l Ltd.,*** [141] the defendants, a company and individuals based in New Zealand, operated websites under domain names that allegedly infringed plaintiff's trademarks. The court found that the content of the website reflected the defendants' intention to target the U.S. market. In reaching that result, the court relied on the facts that **(1)** defendants purposefully went to the United states registrar, NSI, to gen ***'.com'*** domain name, rather than staying at home and registering a ***'county-specific .nz'*** domain; **(2)** the website featured banner advertisements from ten U.S. companies; some of the ads, when clicked, displayed a page designed for U.S. Consumers; **(3)** defendants quoted advertising rates to prospective advertisers in U.S. dollars; **(4)** the website offered to sell travel packages that were priced in U.S. dollars; and **(5)** the website offered books for sale, in affiliation with Amazon.com, a U.S. company.

Both the aforesaid cases point out that the targeting of the forum state is an important criterion in establishing personal jurisdiction.

1.6 THE EFFECTS TEST AND ONLINE INTERACTION

[140] *Millennium Enterprises Inc v Millennium Music, LP* 33 F Supp 2d 907 (D Or)[1999]
[141] *Quokka Sports, Inc v Cup Int'l Ltd* 99 FSupp 2d 1105 (ND Cal)[1999]

Another criterion that has been accepted by the courts has been the ***"Effects"*** of online interaction on the forum state. The US Supreme Court in ***Calder vsJones,***[142] held that the minimum contacts due process requirement may be satisfied on the basis of the effects that out-of-state conduct has in the forum state. In that 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 plaintiff resided in California. The Court reasoned that the defendants had engaged in *'international, 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 effect 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: **(1)** intentional actions **(2)** expressly aimed at the forum state **(3)** causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state.[143]

What separates the effect test from other personal jurisdiction approaches is that the focus is on the ***knowledge*** or ***likelihood*** of causing harm in the forum state. All the previous approaches put more focus on the level of either online or online as well as offline interactions. That's why more and more cases involving defamation or infringement of intellectual property rights have been decided on the basis of this test. For example, in ***Telco Communications vs An Apple a Day,***[144] (The Virginia plaintiff sued the Missouri defendant for, inter alia, defamation in Internet press releases from which the plaintiff's stock prices suffered. The court held the exercise of jurisdiction to comport with due process since the defendant knew the statements would be damaging to the plaintiff and was aware of the location of the plaintiff in Virginia); ***PurCo Fleet Services, Inc. vs Towers,***[145] (defendant registered domain name corresponding to plaintiff's trademark, and set up website that forwarded visitors to its own site); ***3DO Co vsPoptop Software Inc.,***[146] (defendant's website allowed visitors to download software that allegedly

[142] *Calder vs Jones* 456 US 783 [1984]
[143] Full text of "final_paper1_(v1i2)" - archive.org <https://archive.org/stream/Final_paper1_v1i2/final_paper1_(v1i2)_djvu.txt>
[144] *Telco Communications v An Apple a Day* Civ Act No 97-542-A (E D Va) [1997]
[145] *PurCo Fleet Services, Inc v Towers* 38 F Supp 2d 1320 (D Utah)[1999]
[146] *3DO Co vPoptop Software Inc* 49 USPQ 2d (BNA) 1469 (ND Cal)[1998]

infringed plaintiff's copyright and misappropriated plaintiff's trade secrets); ***Bunn-O-Matic Corp vs Bunn Coffee Service, Inc.,***[147](defendant's website included terms that allegedly infringed plaintiff's trademarks); ***Digital Equipment Corp vs AltaVista Technology, Inc.,***[148](the court drew an analogy between trademark infringement that occurs on a website and infringement that arrives in the state via other means of communication like telex, telephone, and mail and held that using the Internet under the circumstances of this case is as much knowingly sending into Massachusetts the allegedly infringing and therefore tortious uses of Digital's trademark as is a telex, mail, or telephonic transmission).

The application of the effect test in the online environment is to establish the tortious liability of the defendant and the long-arm reach of the plaintiff's forum state to have personal jurisdiction over such defendants. Similarly in the ***Banyan Tree Holding (P) Ltd vs A. Murali Krishna Reddy,***[149]the Division Bench of Delhi High Court, it was held that effect test to apply where a forum state is justified in assuming personal jurisdiction over a foreign defendant, plaintiff must plead and show *prima facie* that specific targeting of the forum state by defendant resulted in an injury or harm to the plaintiff in the forum state in which case the forum state, can presume jurisdiction over out of state defendant.

1.7 CONCLUSION

The effect test, like the Zippo test is not free from subjectivity. The issue of jurisdiction is often decided at the threshold of litigation on the pleadings and inferences drawn from the pleadings. The same set of facts that might lead one court to conclude that a defendant intended purposefully to cause an effect within a given jurisdiction might not lead another court to the same conclusion. Targeting to some courts simply connotes an effort specifically to reach a person who resides in the forum, rather than to generate an impact there. To other courts, it may only connote that effects within the forum were foreseeable. In the end, the cases suggest that predictability of outcome is perhaps only marginally greater under the effects test than under the sliding scale test.

[147]*Bunn-O-Matic Corp v Bunn Coffee Service, Inc* 46 USPQ 2d (BNA) 1375 (CD Ill)[1998]
[148]*Digital Equipment Corp v AltaVista Technology, Inc*960 F Supp 456 (D Mass) [1997]
[149]*Banyan Tree Holding (P) Ltd v AMurali Krishna Reddy* Judgment dated 23-11-2008 passed in CS (OS) No. 894/2008

1.8 LET'S SUM UP

In this chapter, we have studied the tests and interaction under cyber law. We discussed the sliding scale approach along with the Interactivity in online as well as offline with a plethora of case laws. We also discussed the effects test and online interaction with respect to it. Finally, we ended the discussion with a comparison between effects test, sliding scale test and forum state targeting and the courts view on it.

1.9 FURTHER READING

- Geist,M. (2001).Is There a There There: Towards Greater Certainty in Internet Jurisdiction, 16 Berkeley Tech.L.J. 1345.
- Rice, D. (2002). Refining the Zippo Test: New Trends on Personal Jurisdiction for Internet Activities. The Computer & Internet Lawyer. Prentice Hall Law& Business.
- Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., &Schiano, W. (2003). CyberLaw: Text and cases (2nd ed.). South-Western College/West. ISBN-10: 0324164882, ISBN-13: 978-0324164886.
- Adeika, John. (2015). Cyberlaw - Standard and Legal Issues.10.13140/RG.2.1.3800.5605.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of Sliding Scale Approach?

The sliding scale approach classifies the websites on the basis of interactivity.

2) What is the Effect Test?

The effect 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: **(1)** intentional actions **(2)** expressly aimed at the forum state

(3) causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state.

3) Describe the case Millennium Enterprises Inc. vs Millennium Music, LP?

In ***Millennium Enterprises Inc. vs Millennium Music, LP,*** the plaintiff which operated music stores in Oregon under the name *'Music Millennium,'* claimed that defendant violated its trademark in that name by operating in South Carolina under the name *'Millennium Music'*. Defendant's website allowed visitors to purchase compact disks, join a discount club, and request franchising information, but no residents of Oregon had made any purchases via the website or engaged in any online communication with the defendant. The court rejected the view that potential interactivity is sufficient to satisfy due process. It held that there must, in addition, be some *'deliberate action'* with the forum state, consisting of either transaction with residents of the forum state or other conduct purposefully directed at them. The court opined, 'Until transactions with Oregon residents are consummated through defendants' Website, defendants cannot reasonably anticipate that they will be brought before this court'.

1.11 ACTIVITY

Differentiate between sliding scale approach, Forum State Targeting and the Effects Test with relevant case laws? (1000-1500 words)

Unit 3: Jurisdictional Approaches of Online Contract

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- European approach to personal jurisdiction
- The Brussels Convention
- Rome Convention

1.2 JURISDICTION ON THE BASIS OF ONLINE CONTRACT

Online contracts come with terms of service agreements and disclaimers. These agreements impose restrictions on the users' regarding the choice of law and forum selection. The judicial

view as arrived in ***Bremen vs Zapata Off-Shore Co.,***[150] is that such clauses (forum selection) are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be *'unreasonable'* under the circumstances. This rule applies, under the federal law, both if the clause was a result of negotiation between two business entities, and if it is contained in a form of contract that a business presents to an individual on a take-it-or-leave-it-basis.

1.3 FORUM SELECTION CLAUSES: CLICK-WRAP CONTRACTS

It makes a good legal sense for the online service providers to limit their exposure to one jurisdiction only. Defending lawsuits at multiple locations could be both expensive and frustrating. Thus the online service provider has no other choice but to subject themselves to only one set of the forum and applicable laws only. The user has no other choice, but to accept the service provider's terms of service conditions by clicking an on-screen button that says **"I Agree", "I Accept" or "Yes".**

In ***Groff vs America Online, Inc.,***[151] the plaintiff, an individual in Rhode Island who subscribed to America Online, sued the company in Rhode Island state court, alleging violations of state consumer protection legislation. The process of becoming a member of AOL includes a step in which the applicant must assent to AOL's Terms of Service by clicking on ***"I Agree"*** button. The Terms of Service contains a forum-selection clause which expressly provides that Virginia law and Virginia courts are the appropriate law and forum for the litigation between members and AOL. AOL moved to dismiss this suit from the Rhode Island Superior Court for the improper venue on the ground that a forum selection clause in the parties' contract mandated that the suit be brought in Virginia, where AOL's base of operations was located. The court agreed and dismissed the suit.[152]

The court held that the plaintiff assented to AOL's terms of service online by the click of an "I agree" button. The terms of service included a clause mandating that suits concerning the service be brought in Virginia. AOL customers must first click on an "I agree" button indicating assent to be bound by AOL's terms of service before they can use the service. This button first appears

[150] *Bremen v Zapata Off-Shore Co*407 US 1 (9-10) [1972]
[151] *Groff v America Online, Inc*[1998] WL 307001 (R I Super Ct 1998)
[152] The Origin of Click-Wrap: Software Shrink-Wrap Agreements <https://www.wilmerhale.com/en/insights/publications/the-origin-of-click-wrap-software-shrink-wrap-agreements-march-22-2000>

on a webpage in which the user is offered a choice either to read, or simply agree to be bound by, AOL's terms of service. It also appears at the foot of the terms of service, where the user is offered the choice of clicking either an "I agree" or "I disagree" button, by which he accepts or rejects the terms of service. The court held that a valid contract existed, even if the plaintiff did not known of the forum selection clause:

"Our court stated the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively signed the agreement by clicking "I agree" not once but twice. Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement."

Citing ***Bremen vs Zapata,*** the court looked to whether enforcement of the clause would be unreasonable. It did so by application of a nine-factor test, including such criteria as the place of execution of the contract, the public policy of the forum state, location of the parties and witnesses, relative bargaining power of the parties, and the conduct of the parties. The court concluded that enforcement of the clause would not be unreasonable, and so dismissed the case.

Similarly in ***Steven J. Caspi, et al vs The Microsoft Network, L.L.C., et al.,***[153] the user could not use Microsoft Network unless she clicked the "I agree" button next to a scrollable window containing the terms of use. Each plaintiff clicked the "I agree" button to use Microsoft Network, indicating their assent to be bound by the terms of the subscriber agreement and thus forming a valid license agreement. The Superior Court of New Jersey held that the forum selection clause contained in Microsoft Network subscriber agreements was enforceable and valid.

It is important to note that in ***Groff vs America Online, Inc.,*** the court had also taken into consideration the "place of execution" of the online contract. It opined, "The place where the transaction has been performed appears to take place where defendant's mainframe is located (Virginia)." and not the place (Rhode Island) when plaintiff clicked the "I Agree" button.

In other words, the courts have also started realizing the location of equipment (computer network) as one of the important elements to assert personal jurisdiction.

[153] *Steven JCaspi, et al v The Microsoft Network, L L C, et al*[1999] WL 462175, 323 NJ Super 118 (NJ App Div, July 2, 1999)

1.4 JURISDICTION BASED ON LOCATION OF A WEB SERVER

Asserting personal jurisdiction based on the defendant's use of IT infrastructure of a service provider, located in the forum state, to host its website may also compel the forum state to exercise its jurisdiction over such defendant.

In ***Jewish Defense Organization, Inc. vs Superior Court,***[154] the plaintiff brought an action for defamation in a California court. Defendants' only relevant contacts with California consisted of contracting with Internet service providers, "located in California," to host a website which they maintained from their residence in New York. The court concluded that the defendant's conduct of contracting, via computer, with Internet service providers, which may be California corporations or which may maintain offices or databases in California, is insufficient to constitute purposeful availment. But in ***3DO Co. vsPoptop Software Inc.,*** the court found it relevant that defendants use a San Francisco-based company as a server to operate a website that distributes allegedly infringing copies of software.

Location of a web server alone cannot be taken as a sufficient cause to constitute purposeful availment. Hosting a website means allotting some space on the webserver. One may have to look into the kind of services provided by the web hosting company and the frequency of their utilization by the web promoter to establish purposeful availment of the forum state where the server is located.

The whole discussion on personal jurisdiction has been able to point out that the courts are beginning to understand the true nature of the website(s). The decisions given by them are more or less based on interpreting the 'revenue' model of the website and the level of interaction it achieved while managing a business transaction. Importantly, the courts have also realized the fact that 'online' business has 'offline' manifestations as well, and it is not prudent to ignore the latter.

Another noticeable feature that has emerged is that 'online' promoter has certain advantages vis-à-vis the user, i.e., in terms of selecting the forum. Location of the webserver has a role to play in deciding the question of personal jurisdiction but again it is the level of interaction between the service provider and the user, which would establish purposeful availment of the forum state.

[154] *Jewish Defense Organization, Inc. v Superior Court*85 Cal Rptr 2d 611 (Cal Ct App)[1999]

1.5 EUROPEAN APPROACH TO PERSONAL JURISDICTION

The European approach to personal jurisdiction in cross-border dispute is rather different from the American approach. The rules determining which country's courts have jurisdiction over a defendant are set out in a regulation issued by the Council of the European Union, known as the Brussels Regulation. This new regulation[155] is an update of a 1968 treaty among European countries, known as the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters.

1.6 THE BRUSSELS REGULATION

The Brussels Regulation, which became effective on March 1, 2002, (the Regulation[156] on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) replaces Brussels Convention of 1968. It is applicable to all European Council countries except Denmark, which will continue to follow the rules of the Brussels Convention and the EFTA countries (Iceland, Liechtenstein, Norway, Switzerland and Poland), where rules of the 1988 Lugano Convention will be applicable.[157]

1.7 APPLICABILITY OF BRUSSELS REGULATION IN ONLINE ENVIRONMENT

The Brussels Regulation has become the established law to resolve disputes concerning jurisdiction and enforcement of judgments in civil and commercial matters. The Regulation is also applicable to resolve online commercial disputes.

On the issue of jurisdiction the Brussels Convention (remained unchanged in the Regulation), sets the rule: Subject to the provisions of this Convention, persons domiciled in a Contracting State shall, whatever their nationality, be sued in the courts of that State (Article 2). Furthermore, A person domiciled in a Contracting State may, in another Contracting State, be sued: in matters

[155]1990 O J (C 189) 2 (consolidated).
[156]Regulation 9EC) No 44/2001 2001 O J 16 January 2001 L 121.
[157]Brussels Convention on Jurisdiction and the Enforcement <https://www.jus.uio.no/lm/brussels.jurisdiction.and.enforcement.of.judgments.in.civil.and.commercial.matters.convention.1968/doc.html>

relating to the contract, in the courts for the place of performance of the obligation in question (Article 5.1). This means that an individual (including a sole trader or partner in a business sued on his own) can be sued where his principal residence is. Article 60 provides that the domicile of a company or other association (including a partnership) is where it has its statutory seat (i.e., its registered office), its central administration or its principal place of business.

From the point of promotions and sale, the Convention says that the consumer may bring proceedings in his own court against a trader if in the state of the consumer's domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising (Article 13), while the Regulation says that the consumer may sue at home if the trader pursues commercial activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State (Article 15).

As websites are generally accessible from anywhere, thus a trader with a website might said to be directing its activities to all EU countries. In case of a dispute, a consumer has a right under Article 15 to take legal action in his or her home court. Any judgment given there would be enforceable in the trader's own country. Article 15 has broadened the scope of traders' liability, as they can now be sued in foreign courts, i.e., for an online trader defending lawsuits at multiple locations could be both expensive and frustrating.[158]

It would be for the European Court of Justice to decide what constituted directed activities. A website may be seen directed to other states if it offers a choice of the languages or currencies of those states, or gives product specifications or delivery times or prices for them. It amounts to a marketing exercise whereby a website is promoting (or targeting) its products or services to consumers in specific EU states.[159]

1.8 ROME CONVENTION

To resolve such cross border consumer contractual disputes, the EU Member States became signatories to the Rome Convention, 1980. It decides which country's law would apply in

[158] Geist, M (2001).Is There a There There: Towards Greater Certainty in Internet Jurisdiction, 16 Berkeley Tech L J 1345

[159]The UK Department of Trade and Industry (DTI) had proposed a way out, that if the website is directed at a particular foreign territory, then the consumer can bring proceedings against the trader in their home state, but if the website is a general site, and not especially directed at the consumer's territory, then trader's own local law would be applicable.

contractual disputes. The Convention gave freedom of choice to the contracting parties: A contract shall be governed by the law chosen by the parties. The choice must be express or demonstrated with reasonable certainty (Article 3.1). It further states that the mandatory rules of the consumer's country of habitual residence will always apply whatever choice of law is made (Article 5).

The Convention further provides that in the absence of choice of law the contract is to be governed by the law of the country with which it is most closely connected (Article 4.1), and it presumes that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has his habitual residence or its central administration (Article 4.2). The performance constitutes the essence of the contract and is generally understood to mean the performance for which the payment is due. It operates by reference to the country where the party who is to affect the characteristic performance has his habitual residence, or, in the case of a company, its central administration.

The Convention contains in Article 5 provisions on consumer contracts, which are similar, though not identical, to those in Article 15 of the Brussels Regulations. It states that: Notwithstanding the provisions of Article 3, a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence (Article 5.2):

- If in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all steps necessary on his part for the conclusion of the contract, or
- If the other party or his agent received the consumer's order in that country, or
- If the contract is for the sale of goods and the consumer travelled from that country to another country and there gave his order, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy.

It is important to note that the mandatory rules of the law cannot be limited or excluded by contractual agreement. They include the rights given to consumers by national legislations.[160] Therefore if the contract meets one of the tests in Article 5.2, the court will apply the law of the consumer's country in deciding the parties' rights and obligations under the contract, regardless

[160]UK on distance selling (e.g., rights to cooling off periods) and the sale of goods (e.g., the right to receive goods, which are of satisfactory quality

of any choice of law to the contrary. It also provides for non-applicability in case of contracts of carriage and contracts for the supply of services, which are to be supplied outside the consumer's country of residence.

1.9 APPLICABILITY OF THE ROME CONVENTION IN ONLINE ENVIRONMENT

Both the Brussels and the Rome Conventions highlight a consumer-oriented Article(s) stating that the consumer may bring proceedings against the trader in the state of the consumer's domicile/habitual residence, if the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising. The questions are – whether these Article(s) are applicable to an online environment also? and does a website promoted by a trader amount to a specific invitation?

Applying the Conventions in an online setting would require an interpretation of the phrase preceded by a specific invitation addressed to him or by advertising i.e., whether an Internet website constitutes advertising in the state of the consumer's domicile. The answer lies in the nature and form of specific invitation.[161]

As far as applicable law is concerned, the courts within the EU apply the Rome Convention even where the applicable law is that of a third country or the parties are not resident or established in the EU.[162]

1.10 LET'S SUM UP

In this chapter, we have studied the jurisdiction on the basis of the online contract along with the concept of jurisdiction based on the location of a web server. We also discussed the European approach to personal jurisdiction, the Brussels regulation and the Rome Convention. Finally, we ended the discussion with the applicability of the aforementioned conventions in the online environment.

[161] Rice, D (2002). Refining the Zippo Test: New Trends on Personal Jurisdiction for Internet Activities.The Computer & Internet Lawyer. Prentice Hall Law& Business

[162]US has not agreed to the Rome and Brussels Convention

1.11 FURTHER READING

- Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000 and November 22, 2000, No RG:00/0538 (Fr.).
- Thomas Schultz, Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface, 19 EUR. J. INT'L L. 779 (2008).
- C. Douglas Floyd &ShimaBaradaran-Robison, Toward a Unified Test of Personal Jurisdiction in an Era of Widely Diffused Wrongs: The Relevance of Purpose and Effects, 81 IND. L.J. 602, 659 (2006).
- Piltz I. (January 22, 2008). Internet law - European Union's Convention on Cyber Crime (ets no. 185): First International Treaty on Crimes Committed via the Internet. Retrieved from http://www.crime-research.org/news/22.01.2008/3144/

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is forum selection clauses based on clickwrap contracts?

Defending lawsuits at multiple locations could be both expensive and frustrating. Thus the online service provider has no other choice but to subject themselves to only one set of the forum and applicable laws only. The user has no other choice, but to accept the service provider's terms of service conditions by clicking an on-screen button that says **"I Agree", "I Accept" or "Yes".**

2) Explain the European approach of Personal Jurisdiction?

The European approach to personal jurisdiction in cross-border dispute is rather different from the American approach. The rules determining which country's courts have jurisdiction over a defendant are set out in a regulation issued by the Council of the European Union, known as the Brussels Regulation. This new regulation[163] is an update of a 1968 treaty among European

[163] 1990 O.J. (C 189) 2 (consolidated).

countries, known as the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters.

3) What is the Brussels Convention?

The Brussels Regulation, which became effective on March 1, 2002, (the Regulation[164] on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) replaces Brussels Convention of 1968. It is applicable to all European Council countries except Denmark, which will continue to follow the rules of the Brussels Convention and the EFTA countries (Iceland, Liechtenstein, Norway, Switzerland and Poland), where rules of the 1988 Lugano Convention will be applicable.

4) What was the reason behind the enforcement of the Rome Convention?

To resolve such cross border consumer contractual disputes, the EU Member States became signatories to the Rome Convention, 1980. It decides which country's law would apply in contractual disputes. The Convention gave freedom of choice to the contracting parties: A contract shall be governed by the law chosen by the parties. The choice must be express or demonstrated with reasonable certainty (Article 3.1).

1.13 ACTIVITY

Explain the European Approach to Personal Jurisdiction along with the Brussels and Rome Convention? Also, elucidate the applicability of both the convention with relevant case laws? (1000 – 1500 words)

[164]Regulation 9EC) No 44/2001 2001 O.J. 16 January 2001 L 121.

Unit 4: Basics of Jurisdiction and Indian Approach

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Jurisdiction based on forum of choice
- Jurisdiction based on CPC
- Cause of action and Contractual obligations

1.2 INDIAN APPROACH TO PERSONAL JURISDICTION

It is within the power of the Indian courts to grant an injunction or anti-suit injunction[165] to a party over whom it has personal jurisdiction, in an appropriate case. This is because of courts of

[165]When a court restraints a party to a suit/proceeding before it from instituting or prosecuting a case in another court including a foreign court, it is called anti-suit injunction.

equity exercise jurisdiction in personam. This power is to be used sparingly as though it is directed against a person, but may cause interference in the exercise of jurisdiction by another court. More so, as the courts have to observe the rule of comity,[166] which states that the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its citizens or of other persons who are under the protection of its law.

Keeping in view the nature of the online commerce involving business-to-business (B2B) or business-to-consumer (B2C) contracts, it is important that the issue of personal jurisdiction should be looked into from all possible sources: **(a)** forum of choice **(b)** civil procedure code, 1908 and **(c)** choice of law.

These sources do not constitute mutually exclusive categories. They are dependent upon each other.

1.3 JURISDICTION BASED ON FORUM OF CHOICE

In fact, the parties may themselves agree beforehand that for resolution of their disputes, they would either approach any of the available courts of natural jurisdiction or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. Thus it is open for a party for his convenience to fix the jurisdiction of any competent court to have their dispute adjudicated by that court alone. In other words, if one or more courts have the jurisdiction to try any suit, it is open for the parties to choose any one of the two competent courts to decide their disputes. In case parties under their agreement expressly agree that their dispute shall be tried by only one of them then the parties can only file the suit in that court alone to which they have so agreed.[167]

The growing global commercial activities gave rise to the practice of parties to a contract agreeing beforehand to approach for resolution of their disputes thereunder either any of the available courts of natural jurisdiction and thereby create an exclusive or non-exclusive

[166] *Hilton vGuyot,* 115 US 113 (163-164) [1995]
[167] *Shriram City Union Finance Corporation Ltd v Rama Mishra,* [2002] 9 SCC 613; [2002] AIR SCW 2617; AIR [2002] SC 2402

jurisdiction in one of the available forums or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. It is the well-settles principle[168] that by agreement the parties cannot confer jurisdiction where none exists, on a court to which CPC applies, but this principle does not apply when the parties agree to submit to the exclusive or non-exclusive jurisdiction of a foreign court. Thus, it is clear that the parties to a contract may agree to have their disputes resolved by a foreign court termed as a neutral court or court of choice creating exclusive or non-exclusive jurisdiction in it.

Significantly, in ***Hakam Singh vs Gammon (India) Ltd.,***[169] the Supreme Court held that where two courts or more have under the Code of Civil Procedure jurisdiction to try a suit or proceeding, an agreement between the parties that the dispute between them shall be tried in one of such courts is not contrary to public policy. Such an agreement does not contravene Section 28 of the Contract Act.

In another significant judgment, the Supreme Court has ruled in ***DhannalalvsKalawativai,***[170] there is no wrong without a remedy ***(Ubi jus ibiremedium).*** Where there is a right, there is a forum for its enforcement. The plaintiff is ***dominuslitis,*** that is, master of, or having dominion over the case. In case of conflict of jurisdiction, the choice ought to lie with the plaintiff to choose the forum best suited to him unless there be the rule of law excluding access to a forum of the plaintiff's choice or permitting recourse to a forum will be opposed to public policy or will be an abuse of the process of law.

It is very much clear from the aforesaid discussion that the forum of choice is discretionary and at the instance of the contractual parties. The parties may submit themselves to the exclusive or non-exclusive jurisdiction of either natural or neutral forum.

1.4 JURISDICTION BASED ON CODE OF CIVIL PROCEDURE

In all civil matter, the Code of Civil Procedure (CPC), 1908, formulates the Indian approach to jurisdiction. Under CPC, one or more courts may have jurisdiction to deal with a subject matter having regard to the location of immovable property, place of residence or work of a defendant

[168] *Modi Entertainment Network v W S G Cricket Pte Ltd,* [2003][4] SCC 341; AIR [2003] SC 1177; [2003] AIR SCW 733
[169] *Hakam Singh v Gammon (India) Ltd*[1971][1] SCC 286; AIR [1971] SC 740; [1971] [2] SCJ 576
[170] *Dhannalal vKalawativai*[2002] 6 SCC 16; [2002] AIR SCW 2873; AIR [2002] SC 2572

or place where the cause of action has arisen. Where only one court has jurisdiction, it is said to have exclusive jurisdiction; where more courts than one have jurisdiction over a subject matter, they are called courts of available or natural jurisdiction.

The jurisdiction of the courts to try all suits of civil nature is very expansive, as is evident from the plain language of section 9 of CPC. This is because of the principle of *Ubi jus ibiremedium*(there is no wrong without a remedy).

1.5 BASIS OF JURISDICTION

To formulate whether the jurisdiction of the courts is exclusive or non-exclusive, in the Internet setting, one must involve the jurisdictional principles as highlighted in the CPC:[171]

a) Pecuniary
b) Subject-matter
c) Territory and
d) Cause of action

Pecuniary jurisdiction limits the power of the court to hear cases up to a pecuniary limit only. As Section 6 provides, nothing herein contained shall operate to give any Court jurisdiction over suits the amount or value of the subject matter of which exceeds the pecuniary limits (if any) of its ordinary jurisdiction.

It is important to note that subject to the pecuniary or other limitations prescribed by any law, and jurisdiction also depends on where subject-matter situate (section 16), where a suit is for compensation for wrong done to the person or movable property (section 19) or where defendants reside or cause of action arises (section 20).

Section 19 of CPC states, where a suit is for compensation for wrong done to the person or movable property, if the wrong was done within the local limits of the jurisdiction of one court and the defendant resides, or carries on business, or personally works for gain, within the local limits of the jurisdiction of another court, the suit may be instituted at the option of the plaintiff in either of the said Courts.

[171] Michaels, Ralf (2016) Jurisdiction, Foundations

Section 20 of CPC states, every suit shall be instituted in a Court within the local limits of whose jurisdiction[172] –

a) The defendant, or each of the defendants where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain; or
b) Any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides or carries on business, or personally works for gain, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carry on business, or personally work for gain, as aforesaid acquiesce in such institution; or
c) The cause of action, wholly or in part arises.

(Explanation) – A corporation shall be deemed to carry on business at its sole or principal office in (India) or, in respect of any cause arising at any place where it has subordinate office, at such place.

On one hand, the Section 19 gives an option to the plaintiff to institute the suit at any of the available courts of natural jurisdiction and thus creating an exclusive jurisdiction in one of the available forums, whereas on the other hand, the principle behind the provision of Clauses (a) and (b) of section 20 is that the suit be instituted at a place where the defendant is able to defend the suit without undue trouble. Also, the essential notion of a business, as contemplated by section 20 is that it is commercial in character. The expression ***'carries on business'*** has a commercial flavour and envisages a commercial enterprise.

In ***Gupta Sanitary Stores vs Union of India,***[173] noticing the gamut of law on the point, AvadhBihariRohtagi, J., as His Lordship then was, speaking for self and for SS. Chadha and G.C. Jain, JJ. of this Court, while interpreting the expression carries on business summed up the legal position in the following terms:

[172]'Suit Can Be File Where Both The Parties Decided The Jurisdiction As Per Contract - Legal News / Law News & Articles - Free Legal Helpline - Legal Tips : Legal India' (*Legal News / Law News & Articles - Free Legal Helpline - Legal Tips : Legal India*, 2020) <https://www.legalindia.com/suit-can-be-file-where-both-the-parties-decided-the-jurisdiction-as-per-contract/>

[173]*Gupta Sanitary Stores v Union of India* AIR [1985] Del 122 (FB)

"I take the test to be this: What is the nature and purpose of the activity in question? If it is commercial, the suit can be filed at the principal place of business or principal office. And also at the place where the cause of action arises wholly or in part.[174]

In most cases where the business is not of a commercial nature the suit must be filed against the government at the place where the cause of action arises wholly or in part. For example, if the contract is entered into at Calcutta, the Courts at Calcutta will have the Jurisdiction.[175]

It is significant to note that the expression 'cause of action' has not been defined in the Civil Procedure Code, 1908. It may be referred to as the facts, which give a person the right to seek judicial relief. In ***Rajasthan High Court Advocates' Association vs Union of India,***[176] the Supreme Court held that the expression 'cause of action' has acquired a judicially settled meaning Compendiously the expression means every fact, which would be necessary for the plaintiff to prove, if traversed, in order to support his right to the judgment of the Court. Every fact, which is necessary to be proved, as distinguished from every piece of evidence, which is necessary to prove each fact, comprises in 'cause of action'. It has to be left to be determined in each case as to where the cause of action arises.

1.6 CAUSE OF ACTION AND CONTRACTUAL OBLIGATIONS

The expression 'cause of action' signifies that bundle of facts, which the petitioner must prove, if traversed, to entitle it to a judgment in its favour by the Court. One can find a better answer to aforesaid plea in relation to 'cause of action' by referring to a decision of the Apex Court in the case of ***Oil & Natural Gas Commission vsUtpal Kumar Basu.***[177]It was a case where the petitioner learnt about tenders being invited for a particular project at Hazira in Gujarat from advertisements appearing in the Times of India in circulation in West Bengal by reading it at Calcutta, submitted its offer from Calcutta, made representations and also sent fax messages from Calcutta and received reply thereto at Calcutta. A writ petition was filed

[174]Also see, *Shri Ram Rattan Bhartia v Food Corporation of India*, [1978] Raj LR 177; ILR [1978][1] Del 308; AIR [1978] Del 183 (FB)
[175]*Nalanda Ceramic and Industries Ltd v N S Choudhury and Co (P) Ltd,* AIR [1977] SC 2142; [1978] Pat LJR [12]
[176]*Rajasthan High Court Advocates' Association v Union of India*[2001][2] SCC 294; AIR [2001] SC 416; [2001] AIR SCW [1]
[177]*Oil & Natural Gas Commission vUtpal Kumar Basu*[1994][4] SCC 711; [1994] AIR SCW 3287; JT [1994] [6] SC 1

before the Calcutta High Court on the plea of part of the cause of action having arisen at Calcutta. In view of the aforesaid facts, holding lack of jurisdiction on the part of Calcutta High Court, which it had assumed bypassing impugned order while allowing the appeal, the Supreme Court laid down in the following terms:

"…..merely because it read the advertisement at Calcutta and submitted the offer from Calcutta and made representations from Calcutta would not, in our opinion, constitute facts forming an integral part of the cause of action. So also the mere fact that it sent fax messages from Calcutta and received a reply thereto at Calcutta would not constitute an integral part of the cause of action…".

Where the cause of action arises from contract, and the parties have not effectively selected the governing substantive law, the relevant criteria in a choice-of-law analysis are **(1)** the place of contracting, **(2)** the place of negotiation of the contract, **(3)** the place of performance, **(4)** the location of the subject matter of the contract, and **(5)** the location of the parties.

1.7 CHOICE OF LAW

Based on its assessment of the contractual obligations involved, a court will apply the choice-of-law rules to determine what law should be applied? The two choices are: either to apply the law of the forum (lexfori), or to apply the law of the site of the transaction, or occurrence that gave rise to the litigation in the first place (lex loci). It is obligatory to note that the modern theory of Conflict of Laws recognizes and, in any event, prefers the jurisdiction of the state, which has the most intimate contact with the issues arising in the case. Ordinarily, jurisdiction must follow upon functional lines.[178]

Where the parties have not expressly or impliedly selected the proper law, the Courts impute an intention by applying the objective test to determine what the parties would have as just and reasonable persons intended as regards the applicable law had they applied their minds to the question. The judge has to determine the proper law for the parties in such circumstances by putting himself in the place of a "reasonable man". He has to determine the intention of

[178] *SurinderKaurSandhu vHarbax Singh Sandhu*, [1984][1] Crimes 928: [1984][3] SCC 698: AIR [1984] SC 1224 (1226)

the parties by asking himself "how a just and reasonable person would have regarded the problem".

For this purpose the place where the contract was made, the form and object of the contract, the place of performance, the place of residence or business of the parties, reference to the Courts have jurisdiction and such other links are examined by the Courts to determine the system of law with which the transaction has its closest and most real connection.

It is very much clear that the courts do have a judicial right to determine the choice of law by identifying the system of law with which the transaction has its closest and most real connection. There is no bar that the law of a foreign country cannot be applied or an Indian party could not be subject to a foreign jurisdiction. The emphasis is on to select proper law.

1.8 LET'S SUM UP

In this chapter, we have studied the Indian approach to personal jurisdiction along with the jurisdiction based on the forum of choice and Code of Civil Procedure. We also discussed the cause of action and contractual obligations and finally, we ended the discussion with the Choice of law.

1.9 FURTHER READING

- Suryajyoti Gupta, "Civil and Criminal Jurisdiction in the Internet", Indian Bar Review, Vol. 29 (2002) p. 45; See also Lotus Case, (1927) PCIJ Ser A
- G.R. Ferrera and D.S. Lichtenstein, Cyber Law –Text and Cases, USA, 2000, p. 21
- Ashish A. Agnis, "Personal Internet Jurisdiction: A Case of Digital Confusion", Journal of Symbiosis Law College, 2004, p. 67; See also L. Edwards, Law and the Internet: Regulating Cyberspace, p. 48.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) **How the issue of personal jurisdiction should be looked into by the court of law?**

It is important that the issue of personal jurisdiction should be looked into from all possible sources: **(a)** forum of choice **(b)** civil procedure code, 1908 and **(c)** choice of law.

2) **What are the two choices of law?**

The two choices are: either to apply the law of the forum (lexfori), or to apply the law of the site of the transaction, or occurrence that gave rise to the litigation in the first place (lex loci).

3) **What is the meaning of the expression 'cause of action'?**

The expression 'cause of action' signifies that bundle of facts, which the petitioner must prove, if traversed, to entitle it to a judgment in its favour by the Court.

4) **What is the basis of jurisdiction?**

To formulate whether the jurisdiction of the courts is exclusive or non-exclusive, in the Internet setting, one must involve the jurisdictional principles as highlighted in the CPC:

a) Pecuniary
b) Subject-matter
c) Territory and
d) Cause of action

1.11 ACTIVITY

Elucidate the basis of jurisdiction along with jurisdiction based on forum of choice and code of civil procedure with relevant case laws? (1000 words)

Block 4
Freedom of Expression in Cyberspace

Unit 1: Indian Constitutional and Freedom of Expression

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The concept of Reasonable restrictions
- Freedom of expression and the Internet
- Freedom of speech and expression

1.2 INTRODUCTION

The Indian Constitution lays down under Article 19 certain fundamental rights to every citizen. The Art. 19 uses the expression *'freedom'* and mentions the several form and aspects of it, which are secured to individuals, together with the limitations that could be, placed upon them in the general interest of the society.

1.3 REASONABLE RESTRICTIONS

Article 19(1)(a) provides that all the citizens shall have the right to freedom of speech and expression. But it should be read with the sub-Art. (2), which imposes reasonable restrictions imposed by the State relating to **(1)** defamation; **(2)** contempt of court; **(3)** decency or morality; **(4)** security of the State; **(5)** friendly relations with foreign states; **(6)** incitement to an offence; **(7)** public order; **(8)** maintenance of the sovereignty and integrity of India.

Hence a law made in respect of the matters referred to in Art. 19(2) must prima facie be presumed to be constitutionally valid and due weight must be given to the legislative judgment on the questions of reasonableness, though that judgment is subject to judicial review.

According to Seervai, H.M., it is difficult, if not impossible, to read into the words "reasonable restrictions" the test of "clear and present danger"[179] evolved by the US Supreme Court in dealing with the freedom of speech and the press. The difference between the First Amendment of the US Constitution and Art. 19(1)(a) was noted by Douglas J. in ***Kingsley Corporation vs Regents of the University of New York,***[180] in holding that all pre-censorship of cinema films was constitutionally void, he said:

"If we had a provision in our constitution for reasonable regulation of the press such as India has included in here there would be room for argument that censorship in the interest of morality would be permissible".

In other words, the Indian Constitution provides that even freedom of speech must yield to public order, i.e., "liberty with order". It was held by the Supreme Court in ***M.H. Devendrappavs Karnataka State Small Industries Development Corpn:***[181]

"The fundamentals freedoms enumerated under Art. 19 are not necessarily and in all circumstances mutually supportive, although taken together they weave a fabric of free and equal democratic society, e.g., the right to reside and settle in any part of the country can be put in

[179]It is important to note that the test of "clear and present danger" has been rejected by the Supreme Court in *BabulalParate v Maharashtra,* AIR [1961] SC 884: [1961][3] SCR 423: [1961][2] Cr LJ 16
[180]*Kingsley Corporation v Regents of the University of New York*[1959] 360 US 684: [1959][3] L Ed 2d 1522
[181]*M H Devendrappa v Karnataka State Small Industries Development Corpn*[1998][3] SCC 732: AIR [1998] SC 1064: [1998] AIR SCW 850

jeopardy by a vociferous local group freely expressing its view against persons from another part of the country. Freedom of speech of one affects the freedom of movement of another. Some restriction on one's rights may be necessary to protect another's rights in a given situation. The rights must be harmoniously construed so that they are properly promoted with the minimum of such implied and necessary restrictions".

1.4 FREEDOM OF EXPRESSION AND THE INTERNET

Keeping in view the concept of "liberty with order", application of the freedom of expression in the context of the Internet would be a restrictive one. The courts would have to first understand the nature of the Internet medium before selectively applying the reasonable restrictions as set out in Article 19(2).

As it was held in ***K. Narayanan vs State,***[182]that "the freedom of speech and expression guaranteed by Article 19(1)(a) included the freedom to acquire knowledge, to read books and periodicals and read any type of literature, subject only to reasonable restrictions being placed on such rights".

Thus the fundamental right of freedom of speech and expression extends to the Internet medium as well. Every citizen has the freedom to acquire or share knowledge (or information) using the Internet and related resources, subject only to reasonable restrictions. The courts may apply reasonable restrictions in the interest of decency or morality to restrict the publication of information which is obscene in electronic form. For this purpose, the courts may have to invoke reasonable restrictions in the interest of decency or morality in light of sections 67, 67A and 67B of the Information Technology Act, 2000 which deals with publication or transmission of obscene material in electronic form.

Earlier as per the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27Th February, 2003, Indian Computer Emergency Response Team (CERT-In) had been designated as the single authority for issuing of instructions in the context of blocking of websites, as there is no explicit provision in the Information Technology Act for blocking of websites. The aforesaid notification

[182]*K Narayanan v State*AIR [1973] Ker 97 (FB)

was based on the premise that such blocking can be challenged if it amounts to restriction of freedom of speech and expression. However, the websites promoting hate content, slander, or defamation of other, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim the constitutional right of free speech. Blocking of such websites may be equated to "balanced flow of information" and not censorship.

The question is how far the concept of "balanced flow of information" could be stretched. For example, earlier CERT-In attempted to block Meghalaya secessionist email group (groups.yahoo.com/gro-ups/kynhun), and it led to blocking of entire Yahoo Groups site by the overzealous ISPs, with the result complete blackout of communication among the other legitimate users of the Yahoo Groups.

Interestingly, the Central Government has rescinded the aforesaid notification vise Gazette Notification G.S.R. 410(E) dated 17th May 2010. In other words, CERT-In is no longer empowered to block websites or content. The District Court of Delhi in ***Lacoste S.A. vs Ninety Nine Labels (P) Ltd.,***[183] ***Tommy Hilfiger Licencing LLC vs Ninety Nine Labels (P) Ltd.,***[184] and ***Polo Lauren Company vs Ninety Nine Labels (P) Ltd.,***[185] has opined[186] that the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27th February 2003 has been rescinded vide Gazette Notification G.S.R. 410(E) dated 17th May 2010, hence CERT-In is neither a proper or necessary party to block websites or contents thereof. This raises an interesting question – what would be the remedy if someone is aggrieved by defamatory or obscene content?

ILLUSTRATION

Various Options to Block the Content

The following legal options are available to an aggrieved person:

[183] *Lacoste S A v Ninety Nine Labels (P) Ltd*TM No 310/2013
[184] *Tommy Hilfiger Licencing LLC v Ninety Nine Labels (P) Ltd,*TM No 311/2013
[185] *Polo Lauren Company v Ninety Nine Labels (P) Ltd* TM No 312/2013
[186] Vide order dated 23-7-2014.

1) Approach the Grievances Officer as per procedure laid down the Information Technology (Intermediary Guidelines) Rules 2011 and seek directions related to blocking or removal of such content, or
2) Approach the court and seek directions against intermediaries publishing or hosting such content, or
3) Approach the designated Nodal Officer of Ministries or Departments of Government of India or State Governments or any agency of the Central Government with a request that content falling under the provisions of section 69A need to be blocked for public access; Such officer is then to request the Group Coordinator, Cyberlaw Division, Ministry of Communications & Information Technology as per the procedure laid down under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

It is important to note that any censorship is a temporary step, as the 'blocked content' could easily be accessed as cached material via web search. Imposing "reasonable restrictions" on the Net has certain limitations. This fact needs to be appreciated, and accordingly, a legal framework based on the principle of "reasonableness and due care" has to be adopted. This question was examined by the Supreme Court in series of Writ Petitions, like ***ShreyaSinghalvs Union of India,***[187]***Dilip Kumar Tulsidas Shah vs Union of India,***[188] ***Rajeev Chandrashekharvs Union of India,***[189] ***Common Cause (A Regd. Society) vs Union of India,***[190] ***PUCL vs Union of India,***[191] ***Mouthshut.com (India) Pvt. Ltd vs Union of India,***[192]***TalimaNasrinvs State of Uttar Pradesh,***[193]***ManojOswalvs Union of India,***[194] ***and Internet and Mobile Association of India vs Union of India.***[195]As articulated previously, the question before the court was whether section 66A (Punishment for sending offensive messages through communication service, etc.) of the Information Technology Act was violative of Article 14, 19 and 21 of the Constitution of India? The Court declared section 66A as ultra vires on account of causing chilling effect.

[187]*ShreyaSinghal v Union of India*WP (Crl) No 167 of 2012
[188]*Dilip Kumar Tulsidas Shah v Union of India*WP (C) No 97 of 2013
[189]*Rajeev Chandrashekhar v Union of India*WP (C) No 23 of 2013.
[190]*Common Cause (A Regd Society) v Union of India*WP (C) No 21 of 2013
[191]*PUCL v Union of India*WP (C) No 199 of 2013
[192]*Mouthshut.com (India) Pvt Ltd vUnion of India*WP (C) No 217 of 2013
[193]*TalimaNasrin v State of Uttar Pradesh*WP (Crl) No 222 of 2013
[194]*ManojOswal v Union of India*WP (Crl) No 225 of 2013
[195]*Internet and Mobile Association of India v Union of India*WP (C) No 758 of 2014

The relevant extract of the Supreme Court judgment in ***ShreyaSinghal case*** referring to section 66A being violative of freedom of speech and expression is reproduced for better understanding of the judicial interpretation of Article 19 protecting freedom of speech and expression over Internet.

1.5 FREEDOM OF SPEECH AND EXPRESSION

The Preamble of the Constitution of India inter alia speaks of liberty of thought, expression, belief, faith and worship. It also says that India is a sovereign democratic republic. It cannot be overemphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme.

Various judgments of this Court have referred to the importance of freedom of speech and expression both from the point of view of the liberty of the individual and from the point of view of our democratic form of government. For example, in the early case of ***RomeshThapparvs State of Madras,***[196] this court states that freedom of speech lay at the foundation of all democratic organizations. In ***Sakal Papers (P) Ltd. vs Union of India,***[197] a Constitution Bench of this Court said freedom of speech and expression of opinion is of paramount importance under a democratic constitution which envisages changes in the composition of legislatures and governments and must be preserved. In a separate concurring judgment Beg.J.said, in ***Bennett Coleman & Co. vs Union of India,***[198]that the freedom of speech and the press is the Ark of the Covenant of Democracy because public criticism is essential to the working of its institutions.

Equally, in ***S. Khushboovskanniamal,***[199] this court stated, in paragraph 45, that the importance of freedom of speech and expression though not absolute was necessary as we need to tolerate unpopular views. This right required the free flow of opinions and ideas essential to sustain the collective life of the citizenry. While an informed citizenry is a pre-condition for meaningful governance, the culture of open dialogue is generally of great societal importance.

[196] *RomeshThappar v State of Madras*[1950] SCR 594 [602]
[197] *Sakal Papers (P) Ltd v Union of India*[1962] 3 SCR 842 [866]
[198] *Bennett Coleman & Co v Union of India*[1973] 2 SCR 757 [829]
[199] *S Khushboo vkanniamal*[2010] 5 SCC 600

Justice Brandeis, in his famous concurring judgment in ***Whitney vs California,***[200] said:

"Those who won our independence believed that the end of the state was to make men free to develop their faculties and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty. They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile; that with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty; and that this should be a fundamental principle of the American government. They recognized the risks to which all human institutions are subject. But they knew that order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies; and that the fitting remedy for evil counsels is good ones. Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law-the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.

Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears. To justify suppression of free speech, there must be reasonable ground to fear that serious evil will result if free speech is practised. There must be reasonable ground to believe that the danger apprehended is imminent. There must be reasonable ground to believe that the evil to be prevented is a serious one.[201] Every denunciation of existing law tends in some measure to increase the probability that there will be a violation of it. Condonation of a breach enhances the probability. Expressions of approval add to the probability.

[200] *Whitney v California*71 L Ed 1095
[201] *Whitney v. California* | US Law | LII / Legal Information <https://www.law.cornell.edu/supremecourt/text/274/357>

Propagation of the criminal state of mind by teaching syndicalism increases it. Advocacy of lawbreaking heightens it still further.[202] But even advocacy of violation, however reprehensible morally, is not a justification for denying free speech where the advocacy falls short of incitement, and there is nothing to indicate that the advocacy would be immediately acted on. The wide difference between advocacy and incitement, between preparation and attempt, between assembling and conspiracy, must be borne in mind. In order to support a finding of the clear and present danger, it must be shown either that immediate serious violence was to be expected or was advocated, or that the past conduct furnished reason to believe that such advocacy was then contemplated."

This leads us to a discussion of what is the content of the expression "freedom of speech and expression". There are three concepts which are fundamental in understanding the reach of this most basic of human rights. The first is discussion, the second is advocacy, and the third is incitement. Mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart of Article 19(1)(a).[203] It is only when such discussion or advocacy reaches the level of incitement that Article 19(2) kicks in. It is at this stage that a law may be made curtailing the speech or expression that leads inexorably to or tends to cause public disorder or tends to cause or tends to affect the sovereignty & integrity of India, the security of the State, friendly relation with foreign States, etc. Why it is important to have these three concepts in mind is because most of the arguments of both petitioners and respondents tended to veer around the expression "public order".

1.6 LET'S SUM UP

In this chapter, we have studied the concept of reasonable restrictions with respect to Article 19 of the Indian Constitution along with the Freedom of Expression and the Internet. We also discussed the concept with a plethora of case laws and finally we ended the discussion with Freedom of Speech and Expression.

[202]Brandeis Concurring With Holmes in *Whitney v. California* <https://firstamendmentwatch.org/history-speaks-brandeis-concurring-holmes-whitney-v-california-1927/>
[203]Justice Deepak Gupta's speech on sedition law being abused <https://theprint.in/opinion/heres-the-text-of-justice-deepak-guptas-speech-on-sedition-law-being-abused-and-misused/288439/>

1.7 FURTHER READING

- Seervai, H.M., Constitutional Law of India: A Critical Commentary, Vol. 1 (1975), N.M. Tripathi, Bombay.
- *Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79(1) New York University Law Review, 1 (2009).*
- *Eugene Volokh, Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex , (February12, 2011).*
- *Durga Das Basu, Vol. 2, Commentary on the Constitution of India, 2401 (8th edn., 2007).*

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What does Article 19 of the Indian Constitution state?

The Art. 19 uses the expression *'freedom'* and mentions the several form and aspects of it, which are secured to individuals, together with the limitations that could be, placed upon them in the general interest of the society.

2) Sum up the preamble of the Indian constitution?

The Preamble of the Constitution of India inter alia speaks of liberty of thought, expression, belief, faith and worship. It also says that India is a sovereign democratic republic. It cannot be overemphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme.

3) What are the 3 concepts which are fundamental in understanding that reaches to human rights?

The first is discussion, the second is advocacy, and the third is incitement.

4) What is the outcome of ShreyaSinghal case?

The Court declared section 66A as ultra vires on account of causing chilling effect.

1.9 ACTIVITY

Explain the concept of reasonable restrictions along with Freedom of speech and expression with relevant case laws? (1000 words)

Unit 2: Examination of Rights Under Indian Laws

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Status of Freedom of Speech and Expression under Indian Constitution
- Grounds on which laws can be made to impose reasonable restrictions in the exercise of the right of free speech and expression
- Provisions of the Information Technology Act, 2000, which are being used to tackle the problems arising

1.2 INTRODUCTION

Certain rights are given to individuals by mere reason of being born, and freedom of speech and expression is one such right. Freedom of expression is one of the basic principles of liberty,

society as well as a healthy democracy. Various international charters, declarations, conventions like Universal Declaration of Human Rights, International Convention on Civil and Political Rights, European Convention on Human Rights and Fundamental Freedoms, also advocate in support of this right and protect the same.[204] In the Indian legal matrix, this right of freedom of speech and expression finds place as one of the Fundamental Rights under the Indian Constitution, which collectively are known to be one of the parts of the basic structure of our Constitution.

1.3 ANALYZING RIGHT UNDER THE INDIAN LAWS

Under Indian legal regime, the right finds a place under Article 19 (1) (a) and is read with Article 19 (2), where the latter contains the grounds on which the reasonable restrictions on the exercise of the right can be imposed. Article 19 (1) (a) states that "all citizens shall have the right to freedom of speech and expression".

As it is a well-recognized principle of our Constitution that certain fundamental rights are available to only citizens of the country, whereas others are available to all the people irrespective of whether they are the citizens of this country or not. Article 19, as evident from the plain reading itself, is applicable and available to citizens only, and thus non-citizens aren't entitled to the rights encapsulated under Article 19.

However, this right is not absolute in nature and the grounds on which the laws can be made so as to impose reasonable restriction in the exercise of the right of freedom of speech and expression (as given under Article 19 (1) (a)) are given under Article 19 (2).[205] These are:

- Sovereignty and Integrity of India ;
- Security of the State ;
- Friendly relations with foreign States ;
- Public Order ;
- Decency ;

[204] M Yar, Cybercrime and Society SAGE, 2016
[205] RBroadhurst, "Developments in the globallLaw enforcement of cybercrime," Policing: An International Journal of Police Strategies and Management, vol29, no 3, pp 408–433, 200 6 <https://doi.org/10.1108/13639510610684674>

- Morality ; or
- In relation to contempt of court, defamation, incitement to an offence.

Under the IT Act also, the power to block certain websites and computer resources (and thus in a way, curtailment on the right of freedom of speech and expression), has been given to the Central Government. Section 69A of the IT Act empowers the Central Government or any officer specially authorized by it to order any government agency or intermediary to block access, by public, to certain information which is generated by, stored in or transmitted by computer resources) in the interest of the defence of India, its sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order or for preventing incitement to the commission of an offence. Further, the details of the procedural safeguards that need to be followed while blocking access have been mentioned in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (hereinafter referred to as the Blocking Rules).

1.4 ANALYZING DIFFERENT CONCEPTS GIVEN IN SHREYA SINGHAL CASE

One of the points which came up for the consideration of the court was whether the restrictions mentioned under Article 19(2) also apply to speech and expression made with the use of internet, or in the context of freedom of press/media, whether the restrictions apply to electronic media as well. This point came up in the Supreme Court during arguments in the case of *ShreyaSinghal v. Union of India (Writ Petition (Criminal) 167 of 2012)*, and the argument that Article 19(2) doesn't apply to electronic media was rejected by the Hon'ble Supreme Court after placing reliance on its judgment in the case of *Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal,* wherein the Apex Court held that "The 'right to communicate' includes right to communicate through any media that is available whether print or electronic or audiovisual such as advertisement, movie, article, speech etc.". Placing heavy reliance on this previously decided case of the Apex Court, Justice Nariman in the ShreyaSinghal case pronounced that "The virtues of the electronic media cannot become its enemies."[206]

[206] R P Kataria& S K PSrinivasan,Cyber Crimes Law, Practice & Procedure along with Cyber Evidence and Information Technology Act, 2000 with Allied Rules (New ed 2014)

However, when it comes to cyberspace, the Hon'ble Supreme Court did differentiate it with any other medium and upheld that the Internet is a distinct medium. The factors relied on by the court for the same were "global reach of Internet", "impossibility of pre-censorship" (because anyone can publish their content), "possibility of the use of new technologically advanced methods to modulate the content", "lack of code of ethical conduct" and "individualised production" (of the content). And hence the Court affirmed that electronic medium "may warrant a greater regulation over licensing and control and vigilance on the content of the program telecast".

After analyzing and settling on the points above mentioned along with a few others, on the question of validity of Section 66A of the IT Act, 2000, the Supreme Court upheld that the said provision can't be justified as placing reasonable restrictions on the exercise of right on the grounds mentioned under Article 19 (2). The Court then went on to analyse how the provision couldn't be said to be justified under each grounds of Article 19(2). To the best far outreach, out of all the grounds mentioned under Article 19(2), it can be confused to be justified undergrounds of public order, defamation, incitement to an offence, decency and morality and nothing else. The Court refused to accept that the impugned provision would be justified under the interests of 'public order' because the scope of the provision was so large that it covered within its ambit, both messages to individuals as well as mass messages. Then, it refused the impugned provision, the protection under the exception for defamation because the provision didn't concern itself with injury to reputation. For refusing the provision to be considered as a valid exception on the ground of prevention of 'incitement to an offence', the Court gave the reason that it seeks to control all information irrespective of whether it 'incites' anyone or not. Lastly, on the exception on the ground of decency or morality, the court didn't give the provision the defence of the mentioned grounds because the provision made an only oblique reference to those concepts.[207]

While striking down the provision, the Court also pointed out that the language of the provision and also the terminology referred to in Section 66A is vague, undefined and open-ended. For instance, terms like 'annoying', 'inconvenience' and 'grossly offensive' which have been used in the provision do not point to any specific offence and hence creates confusion for both law

[207]Obar, J A and Wildman, S (2015) Social media definition and the governance challenge: An introduction to the special issue. TELECOMMUNICATIONS POLICY, 39(9), 745-750

enforcement agencies and the general public about what is permitted under the then impugned provision and what is not.

In a country like India, which has recently switched on and has started using the internet at a rapid increase, and a lot of people starting to express their views over the internet through blogs, vlogs, social networks, it is a very important decision and is much appreciated. Also, in a societal set up like ours where the precedent has been set in a very negative way which advocates for suppressing the dissent which is against the people at power, this judgment has given the people a lot of moral support and assurance and will encourage people to express their views over the internet without any fear of vengeance.

1.5 INDIAN CYBER LAW AND SOCIAL MEDIA

At present, there is no specific legislation in our country which deals directly with social media. However, several provisions of a bundle of laws which collectively are called cyber laws could be sought for redressal in case of violation of any rights in the cyberspace, internet and social media.[208] Most important of them under the Information Technology Act, 2000 are listed below:-

1. Sections 65, 66, 66A, 66C, 66D, 66E, 66F, 67, 67A and 67B of Chapter XI of the IT Act, 2000, contain punishments for computer-related offences, and they can also be committed through social media, the concerned offences are: tampering with computer source code, committing computer-related offences given under Section 43, sending offensive messages through communication services, identity theft, cheating by personation using computer resource, violation of privacy, cyber terrorism, publishing or transmitting obscene material in electronic form, material containing sexually explicit act in electronic form, material depicting children in sexually explicit act in electronic form, respectively.[209]
2. Under Section 69 of the IT Act, 2000, the Central or a State Government has been given the power to issue directions for interception or monitoring or decryption of any

[208]Soomro, Tariq &Hussain, Mumtaz.(2019). Social Media-Related Cybercrimes and Techniques for Their Prevention.Applied Computer Systems. 24. 9-17. 10.2478/acss-2019-0002
[209]Social Media And Freedom of Speech And Expression <http://www.legalserviceindia.com/legal/article-426-social-media-and-freedom-of-speech-and-expression.html>

information through any computer resource in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, for preventing incitement to commission of any cognizable offence, for investigation of any offence.[210]

3. Section 69A of the IT Act, 2000, grants power to the Central Government to issue directions to block public access of any information through any computer resource on similar grounds.
4. Under Section 69B of the IT Act, 2000, the Central Government has been empowered to issue directions to authorize any agency to monitor and collect traffic data or information through any computer resource for cybersecurity.
5. Section 79 of the IT Act, 2000, deals with the liability of intermediary. An intermediary shall not be liable for any third party information, data or communication link made available or hosted by him if certain conditions mentioned therein are fulfilled.
6. Section 66A of the Information Technology Act, 2000.

   Section 66A was originally inserted with an intention to tackle the twin problems of spam and cyberstalking. However, the provision became widely infamous due to it being used to crack down on online dissent and political criticism. After the judgment in the case of ShreyaSinghal vs. Union of India (AIR 2015 SC 1523), this provision has been declared unconstitutional but for a better understanding and appreciation of the points regarding judgment as discussed above it is important to have a look at the provision itself.

66A. Punishment for sending offensive messages through communication service, etc.-

Any person who sends, by means of a computer resource or a communication device-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

[210] Nikita Barman, Legal Implications of Cyber Crimes on Social Networking Websites, International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015, ISSN 2250-3153 (E-Copy) <http://www.ijsrp.org/research-paper-1215/ijsrp-p4850.pdf>

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with a fine.

Explanation.–For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.[211]

1.6 THE ROAD AHEAD

Due to absence of any specific law to deal the matter in hand, there is a very wide scope of misuse of the laws, and misuse of laws is not something which is alien to our system. Even after Section 66A was struck down and declared unconstitutional by the Hon'ble Supreme Court, there have been instances wherein people sharing jokes, memes, posts, or their views have been booked unjustly.[212] Though there may be a disagreement amongst people as to the reason behind these cases being registered, with some blaming it on the unawareness of the police officials regarding the striking down of Section 66A, while some of them alleging the unfair intentions of the officials and thus making a sham case of sedition or defamation etc., whereas some terming it as a means of political vendetta, but all would agree that whatever might be reason for this misuse, it can definitely be curbed by the coming in force of a proper legislation dealing with the matter specifically.

[211]Seema D Trived, Ms. ChandaniKathad, Analytical Study Of Cyber Threats In Social Networking, Proceedings of International Conference on Computer Science Networks and Information Technology Held on 23rd-24th January 2016, in Pattaya, ISBN: 9788193137338 (http://www.innovativeresearchpublication.com/documents/papers/jan_pattaya%202016/pdf%206.pdf)

[212]DrJyoti Rattan, Bharat's Cyber Laws & Information Technology, Bharat, Fifth Edition, 2015, ISBN: 978-93-5139-240-8

1.7 LET'S SUM UP

In this chapter, we have studied how freedom of speech and expression is analyzed under the Indian Laws along with the different concepts given in ShreyaSinghal Case. We also discussed about the Indian Cyber law and social media concepts and finally, ended the discussion with the road map after striking down Section 66A of the I.T. Act.

1.8 FURTHER READING

- Feldman, David, Civil Liberties and Human Rights in England and Wales, 2nd Edition, Oxford University Press, UK, 2002, at 763.
- Baker C E, Human Liberty and Freedom of Speech, Oxford University Press, London, 1989 at p 73.
- Bernardino, Raul. (2015). The Freedom of Speech in Cyberspace. 10.13140/RG.2.1.1496.0089.
- A. J. Feldman, A. Blankstein, M. J. Freedman, and E. W. Felten, ―Social networking with frientegrity: Privacy and integrity with an untrusted provider.‖, in USENIX Security Symposium, pp. 647–662, 2012.
- E. Novak and Q. Li, ―A survey of security and privacy in online social networks, College of William and Mary Computer Science Technical Report , 2012.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Whether a citizen of Malaysia who has been residing in India for last 10 years, move to Supreme Court for the enforcement of right under Article 19 (1) (a) by way of writ petition?**

Since, in the hypothetical situation given above, the person concerned is a citizen of Malaysia and not of India, and certain Fundamental Rights, one of which is Article 19, is available to citizens only, the person concerned is not entitled to this as a Fundamental Right. And since the High Court or the Supreme Court is approached by way of writ petition for the enforcement of any Fundamental Right, this person cannot move to Supreme Court for enforcement of right under 19(1)(a) by way of the writ petition.

2. **What are the grounds which are mentioned under the Indian Constitution on which a reasonable restriction on the exercise of the right of free speech and expression be placed?**

   The grounds under which reasonable restrictions can be placed in the exercise of the fundamental freedom of speech and expression are covered under Article 19 (2). These grounds are Sovereignty and Integrity of India; Security of the State; Friendly relations with foreign States; Public Order; Decency; Morality; or In relation to contempt of court, defamation, incitement to an offence.

3. **Does International Covenant on Economic, Social and Cultural Rights mention about the right of speech and expression to be ensured by the member/signatory nations?**

   No, the International Covenant on Economic, Social and Cultural Rights doesn't. But, the Universal Declaration of Human Rights and the International Convention on Civil and Political Rights does, under Article 19 of both of them.

4. **Whether intermediary has a joint and several liability for information posted upon its portal?**

   No, as mentioned under Section 79 of the IT Act, the intermediary is absolved of all of its liability if it has complied with certain conditions prescribed and referred to in the provision. The Central Government has made separate rules, known as Information Technology (Intermediaries guidelines) Rules, 2011, which requires to be complied with for it being absolved of the liabilities.

5. **Whether the intention of the legislature to bring Section 66A of the IT Act was to suppress dissent against the government?**

No, intention of the legislature was a noble one. Instead, it was to tackle the twin problems of spam and cyberstalking. However, as per the data available, the provision has majorly been used for satisfying the political vendetta and for suppressing the political dissent.

1.10 ACTIVITY

Write about the incidents where cases against individuals have been filed for writing or sharing posts or messages relating to political issue or angle, provided they must have happened after the Supreme Court declared Section 66A as unconstitutional, and the recent individual updates about all of them. In the light of the same, analyse the provisions which have been misused due to any reason whatsoever. (1000 words)

Unit 3: The Legislative Responses in Cyberspace

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The Legislative responses of cyberspace
- The enactment of Community Decency Act
- The verdicts of different cases and opinions of courts

1.2 INTRODUCTION

With the advent of the Internet, there has been a subtle shift in the law-making as well, i.e., the law is now no longer meant for the man only, it is now for the machines as well. For example, the law has been able to recognize the computer as a tool in criminal activity.

A computer could now be referred to as a 'weapon of offence' as well as a 'victim of crime'. What is being witnessed is – the emergence of cyberspace jurisprudence.

1.3 CYBERSPACE: TO LEGISLATE OR NOT

Internet is an open system of communication with unlimited choices. It has its own culture, which is non-hierarchical, open and dynamic. It is, in fact, anti-thesis of whatever the global society has experienced so far. So, what would be the 'philosophy of cyberspace law'? The primary objective of such a philosophy should be to understand the dynamics of this emerging culture. Also, the lawmakers need to address the issues with an open mind without any preconceived notions, biases and restrictions.

The question that the emerging cyberspace has thrown in is that – does cyberspace need a law? If yes, what should be its parameters? Should the 'new' legislation be just an extension of the 'old' legislation or should it reflect an understanding of the emerging medium? And lastly, what should be the response of the courts in safeguarding citizens' constitutional guarantees via-à-vis the new medium?

1.4 THE LEGISLATIVE RESPONSE I

One of the earliest legislative responses to the development of the Internet was the introduction of the Communications Decency Act, 1996 (CDA) by the US government.

Section 502 of the CDA amended sections 223(a) and (d) of Title 47 of the United States Code (USC). These provisions prohibited the making of obscene or 'indecent' material and its transmission to a minor by means of a telecommunication device, and the use of an interactive computer service to send or display 'patently offensive' material to minors.

Section 223(a), the indecency provision, subjects to criminal penalties of imprisonment of no more than two years, or a fine or both, anyone who:[213]

[213] *American Civil Liberties Union v Reno*, 929 F Supp 824 <https://law.justia.com/cases/federal/district-courts/FSupp/929/824/1812782/>

(1) In interstate or foreign communications, by means of a telecommunications device knowingly

(i) Makes, creates, or solicits, and

(ii) Initiates the transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

(2) Knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity.[214]

Section 223(d), the 'patently offensive' provision, subjects to criminal penalties anyone who:

(1) In interstate or foreign communications knowingly

(A) Uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) Uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such a service placed the call or initiated the communication.

(2) Knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity.

The aforesaid provisions were considered as an unacceptable intrusion into the right to free speech, which is protected by the First Amendment to the US Constitution, which states that the "Congress shall make no law abridging the freedom of speech". Subsequently, the American Civil Liberties Union (ACLU) filed a case challenging the legal validity of the aforesaid

[214] *Reno v. ACLU* | US Law | LII / Legal Information Institute <https://www.law.cornell.edu/supremecourt/text/521/844>

provisions. The case came to known as ***American Civil Liberties Union vs Janet Reno, Attorney-General of the United States***[215] ***(ACLU vs Reno 1).***

1.5 THE VERDICT

THE DISTRICT COURT

The District Court for the Eastern District of Pennsylvania fount that whilst the First Amendment to the Constitution enshrined the principle of freedom of speech, this did not apply to child pornography and 'obscenity' which have 'no constitutional protection'.[216]

The court observed, because of the different forms of Internet communication, a user of the Internet may speak or listen interchangeably, blurring the distinction between speakers and listeners on the Internet. Chat rooms, email and newsgroups are an interactive form of communication, providing the user with the opportunity both to speak and to listen/

It follows that unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in the dialogue that occurs there. The Internet is, therefore, a unique and wholly new medium of worldwide human communication.

Communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident'. A document's title or a description of the document will usually appear before the document itself takes the step needed to view it, and in many cases, the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content.

District Judge Dalzell opined, "The internet is a new medium of mass communication. As such, the Supreme Court's First Amendment jurisprudence compels us to consider the special qualities

[215] *American Civil Liberties Union v Janet Reno, Attorney-General of the United States* 929 F Supp 824 (EDPa)[1996]
[216] *Alliance for Community Media v FCC* 56 F 3d 105 (112) (DC Cir)[1995]

of this medium in determining whether the CDA is a constitutional exercise of governmental power. I conclude that the CDA is unconstitutional and that the First Amendment denies Congress the power to regulate protected speech on the Internet.

The CDA will, without doubt, undermine the substantive, speech-enhancing benefits that have flowed from the Internet. The diversity of the content will necessarily diminish as a result.

Some of the dialogue on the Internet surely tests the limits of conventional discourse. Speech on the Internet can be unfiltered, unpolished and unconventional, even emotionally charged, sexually explicit and vulgar – in a word 'indecent' in many communities. But we should expect such speech to occur in a medium in which citizens from all walks of life have a voice. We should also protect the autonomy that such a medium confers to ordinary people as well as media magnates.

The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion.

The absence of governmental regulation of Internet content has unquestionably produced a kind of chaos, but as one of the plaintiffs' experts put it with such resonance at the hearing: what achieved success was the very chaos that Internet is. The strength of the Internet is that chaos".

Just as the strength of the Internet is chaos, so strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment Protects".[217]

THE SUPREME COURT

The US government appealed the district court's decision to the Supreme Court, which affirmed, accepting the court's conclusion that 'the CDA places an unacceptably heavy burden on protected speech, and the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise patently invalid unconstitutional provision'. ***Reno vs ACLU,[218] (Reno II).*** It held that, although the government has an interest in protecting children from potentially harmful

[217] Remember the "borderless" Internet? It's officially dead <https://arstechnica.com/tech-policy/2011/11/the-borderless-internet-is-officially-dead/>

[218] *Reno vs ACLU* 521 US 844 [1997]

materials, the CDA pursues that interest by suppressing a large amount of speech that adults have a constitutional right to send or receive.

Justice Stevens opined that:

"The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in prison for each act of violation. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. As a practical matter, this increased deterrent effect, coupled with the "risk of discriminatory enforcement" of vague regulations, poses greater First Amendment concerns."[219]

"The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in ***Ginsberg and Pacifica,*** the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messaged or displaying them on their own computers in the presence of minors.[220] The general, undefined terms "indecent" and "patently offensive" cover large amounts of non-pornographic material with serious educational or other value".

1.6 THE LEGISLATIVE RESPONSE II

Later in 1998, the US Congress came out with another enactment, the Child Online Protection Act (COPA). It was a second attempt by the Congress to regulate the dissemination to minors of indecent material on the Web/Internet. The "COPA" was signed into law on October 21, 1998.

[219]Washingtonpost.com: Statute 'Silences Some Speakers'
<https://www.washingtonpost.com/wp-srv/national/longterm/supcourt/stories/062797_d.htm>
[220]*Reno v American Civil Liberties Union* : 521 U.S. 844
<https://supreme.justia.com/cases/federal/us/521/844/>

COPA applies broadly on its face to any website that, in the regular course of business, communicates any speech that includes any material that is harmful to minors. COPA defines a person "engaged in the business" as one who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labour to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income).[221]

Under (47 U.S.C. section 231(e)(6)), COPA defines "material that is harmful to minors" as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that[222] –

(A) The average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

(B) Depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) Taken as a whole, lacks serious, literary, artistic, political, or scientific value for minors.

Under COPA, a minor is defined as one under age seventeen. (47 U.S.C. section 231(e)(7)).

COPA also provides Web publishers subject to the statute with affirmative defenses. If a Web publisher "has restricted access by minors to material that is harmful to minors" through the use of a "credit card, debit account, adult access code, or adult personal identification number, a digital certificate that verifies age or by any other reasonable measures that are feasible under available technology," then no; liability will attach to the Web publisher even if a minor should nevertheless gain access to restricted material under COPA. (47 U.S.C. section 231(c)(1)).

[221] Third Circuit Court of Appeals Decision in *ACLU v Reno II*
<https://www.aclu.org/legal-document/third-circuit-court-appeals-decision-aclu-v-reno-ii>
[222] *ASHCROFT vAMERICAN CIVIL LIBERTIES UNION*
<https://www.law.cornell.edu/supct/html/00-1293.ZO.html>

COPA violators face both criminal (maximum fines of $50,000 and a maximum prison term of six months, or both) and civil (fines of up to $50,000 for each day of violation) penalties. (47 U.S.C. section 231(a)(2)).

1.7 THE VERDICT

THE DISTRICT COURT

On the very next day of signing of COPA, i.e., on October 22, 1998, plaintiffs (ACLU et al) filed this suit in the United States District Court for the Eastern District of Pennsylvania, alleging, inter alia, that COPA violated the First Amendment to the Constitution. Plaintiffs sought an injunction to prevent its enforcement. The case came to known as ***American Civil Liberties Union vs Janet Reno, Attorney-General of the United States,***[223] ***ACLU vs Reno (Reno III).***

On February 1, 1999, following an evidentiary hearing, the district court preliminarily enjoined enforcement of COPA, which imposes severe criminal and civil sanctions on persons who by means of the World Wide Web, make any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." (47 U.S.C. section 231(a)(1)-(3)).

The majority of factual findings and conclusions by the district court mirror those found in ***American Civil Liberties Union v Reno (Reno I).*** It held that it would be prohibitively expensive for some commercial speakers who have websites to verify that their users are adults. These limitations must inevitably curtail a significant amount of adult communication on the Internet. Further, it held that respondents were likely to succeed on their claim as COPA violated the First Amendment. "COPA imposes a burden on speech that is protected for adults," and because the government could not prove that COPA is the least restrictive means available to achieve the goal of restricting the access of minors too (harmful to minors) material.

THE COURT OF APPEALS

[223] *American Civil Liberties Union v Janet Reno, Attorney-General of the United States* 31 F Supp 2d 473 (E D Pa)[1999]

Against the district court's order, in ***Reno III,*** the appellant (Reno) moved to the US Court of Appeals for the Third Circuit ***(American Civil Liberties Union vs Reno, (Reno IV)).***[224]On June 22, 2000, the court upheld the granting of injunction on the basis of likely unconstitutionality.

The court of appeals did not reject the district court's rationale, but rather held that "because the standard by which COPA gauges whether material is 'harmful to minors' is based on identifying 'contemporary community standards' the inability of Web publishers to restrict access to their websites based on the geographic locale of the site visitor, in and of itself, imposes an impermissible burden on constitutionally protected First Amendment speech."

The Court of Appeals concluded that COPA's use of "contemporary community standards" to identify material that is harmful to minors rendered the statute substantially overbroad. Because "Web publishers are without any means to limit access to their sites based on the geographic location of particular Internet users," the Court of Appeals reasoned that COPA would require "any material that might be deemed harmful by the most puritan of communities in any state" to be placed behind an age or credit card verification system. Hypothesizing that this step would require Web publishers to shield "vast amounts of material," the Court of Appeals was "persuaded that this aspect of COPA, without reference to its other provisions, must lead inexorably to a holding of a likelihood of unconstitutionality of the entire COPA statute."[225]

THE SUPREME COURT

The US Supreme Court granted the Attorney General's petition for ***certiorari,*** to review the Court of Appeals' determination that COPA likely violates the First Amendment because it relies, in part, on community standards to identify material that is harmful to minors, and now vacate the Court of Appeals' judgment.

CASE	COURT	LEGISLATION IN QUESTION	VERDICT
American Civil Liberties Union,	The District Court for the Eastern District of	Communications Decency Act, 1996	The CDA is unconstitutional and

[224]*American Civil Liberties Union v Reno*217 F 3d 162 (CA) 3 [2000]
[225]Indecency Online | Freedom Forum Institute <https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/indecency-online/>

(ACLU) vs Janet Reno, Attorney-General of the United States (Reno I)	Pennsylvania.	(CDA)	that the First Amendment denies Congress the power to regulate protected speech on the Internet.
Reno vs ACLU, (Reno II)	US Supreme Court	Communications Decency Act, 1996	The CDA suppresses a large amount of speech that adults have a constitutional right to send or receive. It is patently invalid and unconstitutional.
ACLU vs Reno (Reno III)	District Court for the Eastern District of Pennsylvania	The Child Online Protection Act, 1998 (COPA)	The COPA imposes a burden on speech that is protected for adults. The court preliminarily enjoined enforcement of COPA.[226]
ACLU vs Reno (Reno IV)	US Court of Appeals for the Third Circuit.	The Child Online Protection Act, 1998 (COPA)	COPA's use of contemporary community standards to identify material that is harmful to minors rendered the statute substantially overbroad.

[226]First Amendment wins another round online | Salon.com <https://www.salon.com/1999/02/02/feature_232/>

1.8 LET'S SUM UP

In this chapter, we have studied the legislative responses of cyberspace along with the enactment of community decency act, 1996. We discussed the act with case laws along with verdicts and opinions of different courts. Finally, we ended the discussion with a brief of all the cases discussed along with the findings of the court.

1.9 FURTHER READING

- U.S. Department of Commerce, National Telecommunications and Information Administration, A Nation Online: How Americans Are Expanding Their Use of the Internet at 1, 13 (Feb. 2002)
- National Center for Education Statistics, Internet Access in U.S. Public Schools and Classrooms: 1994-2001 at 3 (September 2002).
- Corporation for Public Broadcasting, Connected to the Future (March 2003).
- See In the Matter of Federal-State Joint Board on Universal Service, Children's Internet Protection Act, CC Docket No. 96-45, Order, FCC 03-188 (rel. July 24, 2003) (implementation timing modifications).
- Davidson, Julia & Justice, Patrick & Prevention, South & Institute, Society & Kingdom, United & Davison, Patrick & America, United & Asia, Emma & Kingdom, Majida&Razai, Sara &Scally, Mia & (Australia, Dr. (2016). Child Online Protection in the MENA Region. 10.13140/RG.2.2.36165.65761.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the earliest development of the Internet?

One of the earliest legislative responses to the development of the Internet was the introduction of the Communications Decency Act, 1996 (CDA) by the US government.

2) **How is the word indecency has been defined under the Communications Decency Act?**

Section 223(a), the indecency provision, subjects to criminal penalties of imprisonment of no more than two years, or a fine or both.

3) **What was the enactment that was brought to light by the US Congress?**

In 1998, the US Congress came out with another enactment, the Child Online Protection Act (COPA).

4) **How does COPA define material that is harmful to minors under the act?**

COPA defines "material that is harmful to minors" as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene.

1.11 ACTIVITY

Elucidate the legislative responses of cyberspace with different case laws and the amendments made? (1000 words)

Unit 4: National Sovereignty and Freedom of Expression

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The fact file of Yahoo! Inc.
- The question before the experts
- The expert opinion and the message from Yahoo!'s case

1.2 INTRODUCTION

It would be really interesting to look into the interplay of law and polity in determining the jurisdictional issues flowing from nationalistic constitutional guarantees'. So far, there have only been few cases highlighting the conflict between nationalistic constitutional guarantees' in the Internet space, i.e., conflict between legislative jurisdiction (or national legislative competence) and personal jurisdiction (or judicial competence) of two different nation-states. The case involving Yahoo! Inc. and organizations dedicated to eliminating anti-Semitism has all such ingredients.

1.3 YAHOO! INC.: THE FACT FILE

Yahoo! is an Internet service provider that operates various Internet websites and services that any computer user can access at *http://www.yahoo.com*.[227] It is an all-purpose portal providing services such as Internet search engine, email, an automated auction site, personal web page hostings, shopping services, chat rooms, and a listing of clubs that individuals can create or join.

Yahoo! services ending in the suffix, ".com," without an associated country code as a prefix or extension use the English language and target users who are residents of, utilize servers based in and operate under the laws of the United States.[228] Yahoo! subsidiary corporations operate Yahoo! sites and services in other nations, including, for example, Yahoo! France, yahoo!India,and Yahoo! Spain. Each of these regional web sites contains the host nations' unique two-letter code as either a prefix or a suffix in its URL (e.g., Yahoo! France is found at *http://www.yahoo.fr*and Yahoo! India at *http://www.yahoo.co.in*). Yahoo!'s regional sites use the local region's primary language, target the local citizenry, and operate under local laws. Any

[227] *Yahoo!, Inc v LICRA* - Tom W Bell <http://www.tomwbell.com/NetLaw/Ch03/YahoovLICRA.html>
[228] Legal Risk Management in Electronic Commerce - Chapter 5 <http://www.legalriskmanagement.net/book/5.html>

computer user with Internet access is able to post materials on many of these Yahoo! sites, which in turn are instantly accessible by anyone who logs on to Yahoo!'s Internet sites.[229]

Yahoo!'s auction site allows anyone to post an item for sale and solicit bids from any computer user from around the globe. Yahoo! records when a posting is made and after the requisite time period lapses sends an e-mail notification to the highest bidder and seller with their respective contact information. Yahoo! is never a part to a transaction, and the buyer and seller are responsible for arranging privately for payment and shipment of goods. Yahoo! monitors the transaction through limited regulation by prohibiting particular items from being sold (such as stolen goods, body parts, prescription and illegal drugs, weapons, and goods violating U.S. copyright laws or the Iranian and Cuban embargos) and by providing a rating system through which buyers and sellers have their transactional behavior evaluated for the benefit of future consumers. Yahoo! informs auction sellers that they must comply with Yahoo!'s policies and may not offer items to buyers in jurisdictions in which the sale of such item violates the jurisdiction's applicable laws.

Yahoo! does not actively regulate the content of each posting, and individuals are able to post and have in fact posted, highly offensive matter, including Nazi-related propaganda and Third Reich memorabilia, on Yahoo!'s auction sites.

1.4 THE COMPLAINT

On or about April 5, 2000, La LigueContre Le Racisme Et l'Antisemitisme (The League Against Racism and Antisemitism – "LICRA") sent a "cease and desist" letter to Yahoo!'s Santa Clara headquarters informing Yahoo! that the sale of Nazi and Third Reich related goods through its auction services violate French law. LICRA threatened to take legal action unless Yahoo! took steps to prevent such sales within eight days. Defendants subsequently filed a civil complaint against Yahoo! in the Tribunal de Grande Instance de Paris (the "French Court").[230]

[229]Ibid.
[230]Aditya, S &Yadav, Dr Raj (2015) CYBER LAW: AN ANALYSIS. Plebs Journal of Law 1 69-80

1.5 THE VERDICT I

The French Court found that approximately 1,000 Nazi and Third Reich related objects, including Adolf Hitler's *Mein Kampf, The Protocol of the Elders of Zion* (an infamous anti-Semitic report produced by the Czarist secret police in the early 1900's), and purported "evidence" that the gas chambers of the Holocaust did not exist were being offered for sale on Yahoo.com's auction site. Because any French citizen is able to access these materials on Yahoo.com directly or through a link on Yahoo.fr, the French Court concluded that the Yahoo.com auction site violates Section R645-1 of the French Criminal Code, which prohibits the exhibition of Nazi propaganda and artifacts for sale.

An order was made on May 22, 2000 against the companies Yahoo! France and Yahoo! Inc. by the County Court of Paris in the following terms:[231]

"We order the company Yahoo! Inc. to take all measures to dissuade and make impossible any access via Yahoo.com to the auction service for Nazi objects and to any other site or service that may be construed as constituting an apology for Nazism or contesting the reality of Nazi crimes;

We order the company Yahoo! France to warn any surfer visiting Yahoo.fr, even before use is made of the link enabling him or her to proceed with searches on Yahoo.com, that if the result of any search, initiated either through a tree structure or by means of keywords, causes the surfer to point to sites, pages or forum of which the title and/or content constitutes a violation of French law, as applies to the viewing of sites making an apology for Nazism and/or exhibiting uniforms, insignia or emblems resembling those worn or displayed by the Nazis, or offering for sale objects or works whose sale is strictly prohibited in France, the surfer must desist from viewing the site concerned subject to imposition of penalties provided in French legislation or the bringing of legal action against him".

The French Court set a return date in July 2000 for Yahoo! to demonstrate its compliance with the order.

[231] I N T E R I M C O U R T O R D E R made on 20 November 2000
< http://www.kentlaw.edu/perritt/conflicts/frenchorder.pdf>

1.6 YAHOO'S! RESPONSE

Yahoo! asked the French Court to reconsider the terms of the order, claiming that although it easily could post the required warning on Yahoo.fr, compliance with the order's requirements with respect to Yahoo.com was technologically impossible.

The Yahoo! Inc. pointed out that there was no technical solution, which would enable it to comply fully with the terms of the court order. A panel of experts was then designated to enlighten the Court on the various technical solutions that could be implemented by Yahoo! Inc. in order to comply with its order of May 22, 2000.

1.7 THE QUESTION BEFORE THE EXPERTS

The expert opinion was sought, whether it is possible to:

a) Know the geographical origin and nationality of surfers wishing to access its auctions site.
b) Prevent French surfers or surfers connecting from French territory from perusing the description of Nazi objects posted for auction, and even more importantly to prevent them from bidding.[232]

1.8 THE EXPERT OPINION

The experts filed their opinion on November 6, 2000. They opined that:

a) Some 70% of the IP addresses of French users or users residing in French territory are capable of being correctly identified by specialized providers such as InfoSplit, GeoNet or others, using specialized databases. Around 30% of the IP addresses assigned to French users cannot be identified.

[232] Singh, Harman (2018)Cyber squatting and the Role of Indian Courts: A Review 2 18-23

b) Yahoo! displays advertising banners targeted at surfers considered by that company to be French, and that it, therefore, has the technical means to identify them.

c) In addition to the geographical identification already practiced by Yahoo to target its advertising, it would also be desirable to ask surfers whose IP address is ambiguous to make a declaration of nationality. This declaration, given on honour, would only be required of surfers whose IP address cannot be identified as belonging to a French ISP (e.g. multinational ISPs like AOL, address transmitted from an anonymizersite, or encapsulation of an address assigned by an intranet server).

d) At the discretion of Yahoo, this declaration of nationality could be made on the home page of the auctions site, or only in the context of a search for Nazi objects if the word "Nazi" is included in the user's request, immediately before the search engine processes the request. In these circumstances, the consultants consider that it cannot be reasonably claimed that this would have a negative impact on the performance and response time of the server hosting the Yahoo! auctions service.

e) The combination of two procedures, namely geographical identification of the IP address and declaration of nationality, would be likely to achieve a filtering success rate approaching 90%.

1.9 THE VERDICT II

On November 20, 2000, Jean-Jacques GOMEZ, First Deputy Justice Presiding in the County 00/05308 Court of Paris, reaffirmed its order of May 22, 2000, involving *The League against Racism and antisemitism –LICRA and The French Union of Jewish Students (Plaintiffs) vs Yahoo! Inc. and Yahoo France,*[233]*(Respondents)* and held that Yahoo! to comply with the May 22 order within three months or face a penalty of 100,000 Francs (approximately U.S. $13,300) for each day of non-compliance.[234]

The Court overruled the objection of the respondents that it was not competent to make a ruling in this dispute. It observed that "the simple act of displaying such objects (of Nazi ideology) in France constitutes a violation of Article R645-1 of the Penal Code and therefore a threat to

[233]See <www.cdt.org> for the English translation of the court's order
[234]C JURISDICTION TO ADJUDICATE
<http://www.wneclaw.com/internet/foreignjudgments.pdf>

internal public order; Whereas Yahoo! is aware that it is addressing French parties because upon making a connection to its auctions site from a terminal located in France it responds by transmitting advertising banners written in the French language; Whereas a sufficient basis is thus established in this case for a connecting link with France, which render our jurisdiction perfectly competent to rule in this matter; Whereas any possible difficulties in executing our decision in the territory of the United States, as argued by Yahoo Inc., cannot by themselves justify a plea of Incompetence; Whereas this plea (of not competent) will, therefore, be rejected".

1.10 THE VERDICT III

Yahoo! Inc. or Yahoo France did not go for appeal in France against the aforesaid judgment. Later, Yahoo! Inc. (as Plaintiff) approached the District Court of Northern California for summary judgment with the plea that the French court's order was without effect in the United States since its enforcement would violate Yahoo's First Amendment right of free speech.

It argued that it cannot comply with the French order without banning Nazi-related material from Yahoo.com altogether. Yahoo! Inc. contends that such as ban would infringe impermissibly upon its rights under the First Amendment to the United States Constitution. It sought a declaratory judgment that the French Court's orders are neither cognizable nor enforceable under the laws of the United States. Defendants (LICRA, et al) immediately moved to dismiss on the basis that this Court lacks personal jurisdiction over them. That motion was denied.[235]

Jeremy, Fogel, District Judge observed (November 7, 2001): ***Yahoo! Inc., vs La LigueContre Le Racisme Et l'Antisemitisme a French association, et al***[236]

"This case is not about the moral acceptability of promoting the symbols or propaganda of Nazism. Most would agree that such acts are profoundly offensive. By any reasonable standard of morality, the Nazis were responsible for one of the worst displays of inhumanity in recorded history. This Court is acutely mindful of the emotional pain reminders of the Nazi era cause to Holocaust survivors and deeply respectful of the motivations of the French Republic in enacting the underlying statutes and of the defendant organizations in seeking relief under those statutes. Vigilance is the key to preventing atrocities such as the Holocaust from occurring again.

[235]Dr Gupta &Agarwal, Cyber Laws, Premier Publishing Company, Allahabad, 2010, at pg no 324
[236]*Yahoo! Inc, v La LigueContre Le Racisme Et l'Antisemitisme a French association, et al*145 FSupp 2d 1168, 1179 (N D Cal)[2001]

The Court concluded "that enforcement of the French order by a United States court would be inconsistent with the First Amendment, the factual question of whether Yahoo! possesses the technology to comply with the order is immaterial. Even assuming for purposes of the present motion that Yahoo! does possess such technology, compliance still would involve an impermissible restriction on speech.[237]

1.11 WHAT NEXT?

Undeterred by the verdict given by the District Court of Northern California a group called the Association Amicale des DiportisD'Auschwitz (AADA) filed a criminal case (February, 2002) against Yahoo! Inc. and its former CEO, Tim Koogle for allowing Nazi memorabilia to be sold through their websites thereby justifying war crimes against humanity, in the Tribunal Correctional de Paris.[238]

After the preliminary filing of documents, the trial date was set, January 7, 2003. Under French criminal law, acts committed outside of France by a non-French citizen, which in his home country would not be a violation of its local criminal law, may not be prosecuted before the French courts unless the acts involve crimes against humanity or certain special crimes, such as false declarations by foreigners in foreign Consulates or acts against the State (e.g. espionage or terrorism).

On February 11, 2003, the French criminal court dismissed all charges, holding that Yahoo! Inc. and its former CEO, Tim Koogle, never tried to "justify war crimes (or) crimes against humanity".

1.12 THE MESSAGE

Yahoo! case singularly demonstrates the conflict between legislative jurisdiction (or national legislative competence) and personal jurisdiction (or judicial competence) of the US and France. In the civil case filed by LICRA, the French court aptly applied the private international law as it had a foreign element in the form of display and availability of objects (Nazi memorabilia) hosted by a US-based company (Yahoo! Inc.). This judicial competence (French Court) was well supported by the legislative jurisdiction in the form of an "offence against the collective

[237]Yahoo! Inc, a Delaware Corporation, Plaintiff-appellee
<https://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/>
[238]DrFarooq Ahmad, Cyber Law in India, New Era Law Publication, New Delhi, 2012, pg no 28

memory" (Articles 808 and 809 of the New Code of Civil Procedure) and Section R645-1 of the French Criminal Code, which prohibits the exhibition of Nazi propaganda and artifacts for sale. Similarly, the US Court's view that though "France has the sovereign right to regulate what speech is permissible in France, this Court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders" reflects both legislative and personal jurisdiction (of the US Court).

Also, it was held by the Italian Court of Cassation[239] that loading defamatory information onto a foreign server and displaying its contents on computer screens in Italy constitutes a single actusdelicti of defamation under Article 6 of Italy's Criminal Code, which defines the Code's scope of application as encompassing "all acts or omissions or even the effects of such action or omission which have occurred in whole or in part on Italian territory".

Expressed as a symbol of national sovereignty, the 'freedom of expression' has a different meaning in every nation-state. It is dependent on legislative and personal jurisdiction. Every nation-state has its version of 'freedom of expression'. Hence, it is too early to adopt the "Yahoo!" case as some sort of benchmark.

1.13 LET'S SUM UP

In this chapter, we have studied the essence of Yahoo! case, along with the issues brought before the court of law. We discussed the question that was posed before the experts and the opinion of the experts. Finally, we ended the discussion with the findings of the courts and the outcome of Yahoo!'s case.

1.14 FURTHER READING

- Freeman, R. & Wicks, Andrew &Werhane, Patricia & Mead, Jenny. (2008). Yahoo! And Customer Privacy (a). Darden Business Publishing Cases. 1. 10.1108/case.darden.2016.000356.
- Gautam, Shalini. (2016). Case Study-VERIZON'S YAHOO. The Case Centre.
- Yahoo! Shopping Auctions, Shopping Auctions Guidelines, at http://user. auctions.shopping.yahoo.com/html/guidelines.html (last visited Oct. 14, 2002).

[239] *Attorney General v Unidentified Person*, Judgment 4741, Nov. 17-Dec 27, [2000]

- Bellanger, P. (2011). From sovereignty in general to digital sovereignty in particular. In Les Echos.fr, 54(30). Retrieved from http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221137239/souverainete-general-et-souverainete-numeriq (Accessed 28 February 2012)
- Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. Security Dialogue, 43(1), 3-24.
- Choucri, N., & Clark, D. (2013). Who controls cyberspace? Bulletin of the Atomic Scientists, 69(5), 21-31.

1.15 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the main aim of Yahoo!?

It is an all-purpose portal providing services such as Internet search engine, email, an automated auction site, personal web page hostings, shopping services, chat rooms, and a listing of clubs that individuals can create or join.

2) What are the questions posed before the experts?

The expert opinion was sought, whether it is possible to:

a) Know the geographical origin and nationality of surfers wishing to access its auctions site.

b) Prevent French surfers or surfers connecting from French territory from perusing the description of Nazi objects posted for auction, and even more important to prevent them from bidding.

3) What was the outcome of Yahoo! case?

Yahoo! case singularly demonstrates the conflict between legislative jurisdiction (or national legislative competence) and personal jurisdiction (or judicial competence) of the US and France.

1.16 ACTIVITY

Explain the facts and the verdicts given by different courts in Yahoo!'s case, along with the outcome of the case? (800-1000 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

●