Unit 4: Regulation of Cyberspace: An Overview

Structure

4.0 INTRODUCTION

Internet is not a physical or tangible entity but rather a giant network which interconnects innumerable smaller groups of linked computer networks. The term 'online' (relating to the form of communication

and its mode of transmission by telecommunication lines) can also be used. There has been a rapid increase in the use of the online environment where millions of users have access to internet resources and are providing contents on a daily basis. This content can be accessed from any computer connected to the network though the content may be actually stored on a number of different computers or 'servers' which need not be in the same jurisdiction as the person who is accessing the material. Internet users may be completely unaware where the resource being accessed, is in fact physically located. This computer networking has been very helpful for businesses of all types for a variety of commercial transactions and consumer services. Apart from transactions involving physical goods, delivery of digitized information products such as music, photographs, novels, motion pictures, multimedia works and software can also be done online. In future also it leads to an increase of economic and creative interactions and inevitably also leads to expansion of disputes involving acquisition, use, possession, processing and communication of information.

The rules for regulating business interaction in a country are different from rules for online commerce. Every country in the world is regulated by law, which is the primary source of regulation. Social norms which guide one's behaviour also function as secondary regulatory constraint. The third constraint is the market which regulates through price mechanism by limiting the amount which a person can spend on different needs; another constraint may be the nature of the world in which we exist. In the real world, the person or the entity with whom interaction relating to business is going on can be located; and thereby the validation of a transaction is facilitated. But in Cyber Space it is very difficult, since parties to a transaction may be sitting in adjoining rooms or in distant locations but the network offers no way to know it. It is often argued that cyberspace is unavoidable but it is not regulable, its behaviour can't be regulated. According to Dr. Dan L. Burk, Assistant Professor of Lawseton Hall University, there is simply no coherent homology between Cyberspace and real space, and screening or blocking of Internet resources by country is nearly impossible. On the other hand, it is argued by Lawrence Lessing in his article, 'The Laws of Cyberspace", that Cyberspace has the potential to be the most fully and extensively regulated space that has ever been known – anywhere at any time in our history. According to him just as in real space, behaviour in Cyberspace is regulated by four sorts of constraint i.e., law, social norms, market and codes (also called architecture).

Every technological revolution brings with it a new spate of legal issues and legal problems to be addressed. The real purpose of our study is to stress the need for regulation of Cyberspace and the possibility and scope of its regulation.

4.1 OBJECTIVES

After studying this unit, you should be able to:

- explain the need and desirability for regulation of internet content both in developed and developing countries;
- discuss that in relation to harmful content on on-line services, the greater emphasis is on self-regulatory scheme of industry governance;
- discuss the nation's legal policies and framework for regulating cyberspace;

- state the desirability for international framework of principles, guidelines and rules for global communication; and

- discuss the need for coordinated national, if not international criminal laws to deal with illegal content on online services.

4.2 DESIRABILITY OF REGULATION OF CYBERSPACE

4.2.1 Need for Regulation of Cyberspace

The following reasons can be cited in favor of the above proposition:

1) The most visible and readily sensational concern is about the use of internet particularly for the distribution of obscene, indecent and pornographic content. The use of internet for child pornography and child sexual abuse and the relative ease with which the same may be accessed calls for strict regulation.

2) The challenge that Cyberspace is posing to traditional notions of jurisdiction and regulation is another factor. The increasing business transaction from tangible assets to intangible assets like Intellectual Property has converted Cyberspace from being a mere info space into important commercial space. The attempt to extend and then protect intellectual property rights online will drive much of the regulatory agenda and produce many technical methods of enforcement.

3) With the inventions of new technologies, the media has enhanced the possibility of invasion of the privacy of individual and bringing it into the public domain. The major area of concern where some sort of regulation is desirable is data protection and data privacy so that industry, public administrators, netizens, and academics can have confidence as on-line user.

4) Encryption is the process of converting a message or document into a form which hides the content of the communication from the eyes of an eavesdropping third party and needs to be decrypted if its content is to be read. New cryptographic techniques (cryptography is the process used to encode/encrypt electronic information) are commonly cracked in a relatively short time by computational force or by other analytical means. Therefore, another area in which regulation has assumed importance is in the debate over whether the public should be permitted to use 'cryptography' or not.

5) Internet has emerged as the 'media of the people' as the internet spreads fast there were changes in the press environment that was centered on mass media. Unlike as in the established press, there is no editor in the Internet. In the press and publication environment, editors check the truthfulness of facts and circulate them once the artistic values are confirmed. On the internet however, people themselves produce and circulate what they want to say and this direct way of communication on internet has caused many social debates. Therefore, the future of Cyberspace content demands the reconciliation of the two views of freedom of expression and concern for community standards.

6) Another concern is that, money laundering, be 'serious crime' becomes much simpler through the use of net. The person may use a name and an electronic address, but there are no mechanisms to prove the association of a person with an identity so that a person can be restricted to a single identity or identity can be restricted to a single person. Viruses, rumor-mongering, hate-mail and mail box bombardment are all describable phenomena and because of the fear of retribution all are more likely to use fake identity or may be anonymous mailers rather then a readily identifiable person. Therefore, Cyberspace needs to be regulated to curb this phenomenon.
Please answer the following to check your progress.

Check your progress1 *Spend 3 Min*

Describe the need for regulation of cyberspace?

4.3 HOW CYBERSPACE CAN BE REGULATED

In "Code and other Laws of Cyberspace", Lawrence Lessing argues that the architecture (code) of the internet i.e. The hardware and software of Cyberspace that define the system can be a form of regulation. It is a set of rules implemented or codified in the software by the code writers, requiring the constant certification of identity.

In "A Non delegation doctrine for the digital age" (Cited: 50 Duke L.J. 5), James Boyle argued that regulation of the internet can increasingly rely on a three-fold strategy:

i) Privatization: The state can use a private body to achieve those goals which it could not get directly and then implement that body's decision through mandatory technological arrangements. For e.g. for Copyright enforcement in Cyberspace, the Clinton administrations original plan was to make Internet Service Providers (ISPs) strictly liable for copyright violations by their subscribers – thus creating a private police force, largely free of statutory and constitutional privacy constraints with strong incentives to come up with innovative surveillance and technical enforcement measures.

ii) Propertization: According to him, first of all an attempt is to be made to extend and then protect intellectual property rights online. This will produce many technical methods of enforcement.

iii) Technological Controls the system is to be designed so as to hardware in desired regulatory features. For e.g. Digital texts and music could be encoded to a particular person. Detection devices could be built in to players, so that others cannot play one's music. Unique identifiers could be built into computer chips, so that a person's computer would broadcast a universal ID with an associated set of legal characteristics as you roamed the net.

Blocking software or Internet contents grading system are other forms of regulations based on technology. In Korea, the government has started the internet contents grading system. The system forces the sites designated as 'content harmful to minors' to attach an electronic tag that the blocking

software can catch. Especially the Korean government categories homosexual sites as content harmful to minors and those sites are often blocked.

Please answer the following to check your progress.

Check your progress2: *Spend 2 Min*

Discuss how cyberspace can be regulated.

4.4 LEGAL AND SELF REGULATORY FRAMEWORK

In any country the role of government is seen as the provider of legal and regulatory framework within which its subjects have to function. In this context of regulation of cyberspace, it can be said that the Internets' design precludes central control which may be regulated by government to make the information economy safe, secure, certain and open. Rather in the last few years outstanding progress has been made in identifying appropriate structures for industry self-regulation with the minimum appropriate level of government intervention. The development of technology to permit content labeling and the early growth of complaint hot lines in a number of countries have helped to provide the ingredients for self-regulatory schemes. Here, we will discuss some of the major developments in the area of national and international cooperative, major developments for effective online industry regulation in various countries, and end-user voluntary use of filtering/ blocking technologies. This approach is taken in United Kingdom, Canada, New Zealand and a considerable number of Western European countries.

But the idea that Cyberspace should be presumptively self-governing has resounded in thoughtful scholarship and has been criticized by many scholars and it has been argued that the selective government regulation of Cyberspace is warranted to protect and promote liberal democratic ideas. However, in this unit we will not go into the jurist's debate whether Cyberspace can be self regulated or not but try to find out the possibilities in the existing legal framework in various countries for regulating internet content.

4.4.1 Filtering Devices and Rating Systems

'Filters' are software tools used to block access to unwanted material. By the 1990's, concerns about problematic content on on-line services had prompted the development of a range of content filter software and rating systems including the Platform for Internet Content Selection ('PICS'); for example, E-mail filters automatically deletes the bulk of unread e-mail messages commonly known as 'spam' and can also be customized to delete incoming messages from particular sources. There can be site blocking filters to screen out specified websites or websites containing specified keywords that the system presumes to relate to other objectionable content. Site blocking filters also may use a protocol

'PICS' developed by the World Wide Web Consortium ('W3C') to develop common protocols for the World Wide Web's evolution and ensure its interoperability. Organizations in several countries have established labeling schemes, which conform to the PICS standards, designed for use by parents and schools. For example, RSACI (Recreational Software Advisory Council labeling scheme for the Internet) rating system addresses the level of violence, sex, nudity, and language on a website and operates as a classification of the content on an Internet site rather than making a judgment about its appropriateness for any given audience or purpose. Such an approach has advantages over those filtering programmes that operate on a keyword basis to exclude offensive material but inevitably, a significant amount of useful, inoffensive content is also blocked. However, its major disadvantage is that it is limited to rating functions, rather than more general information. Consequently, it is not adapted to perform more complex information retrieval searches. Other labeling schemes are Safe surf, Cyber Patrol and Surf Watch.

In 1997 W3C created the 'Metadata Activity', which includes the Resource Description Framework (RDF) Working Group. RDF is a protocol for description of Internet content based on a set of 105 'categories' of information, known as the 'Dublin Core', which is used to Filter out obscene content. However, it does not deal with controversial content or aim to protect children from harmful content, but describes those aspects of content such as authorship, publishers, date and source in a similar way to that developed by library catalogues and facilitates more effective searching. Examples of its applications include search engine data collection and digital library collections. Therefore, it has not been widely used as an alternative to those schemes that eliminate content on the basis of controversial content alone (see speech by Gareth Grainger).

Please answer the following to check your progress.

Check your progress 3: *Spend 3 Min*

Describe in brief the legal and self regulatory framework.

4.5 GOVERNMENT POLICIES AND LAWS REGARDING REGULATION OF INTERNET CONTENT

According to Electronic Frontiers Australia (EFA, March 2002) report on government policies regarding internet censorship in various countries, government policies can be classified into the following four categories:

1) The policy to encourage self-regulation.

2) Criminal law penalties (Fines or Jail Terms) applicable to content providers who make content "unsuitable for minors" available online.

3) The government has also mandated blocking of access to content deemed unsuitable for adults; for example: Australia, China, Saudi Arabia, Singapore etc.

4) A number of countries have either prohibited general public access to the internet or require internet users to be a registered / licensed by a government authority before permitting them restricted access.

However, concerns over access to content on internet vary markedly around the world and no universal method can be made applicable to all the Nations. The cyberspace content regulation may depend on technology, law and the cultural concerns in every Nation and is reflected in the respective regulatory law and policies, which we will discuss below.

4.6 UNCITRAL Model Law, 1996

The United Nations Commission on International Trade Law (UNCITRAL) is a Model Law on Electronic Commerce adopted by UN Commission in 1996. with the specific goal to eliminate all kinds of legal and other technical kinds of hindrances and to boost legal certainty for the cyber domain has postulated a series of internationally acceptable rules though it does not regulate every single phase of transactions done electronically. It has embraced the following doctrines:

1) Non discrimination principle: No document can be denied legal enforceability just because it is in electronic means.
2) Technological neutrality principle: Adapting to existing laws which are neutral in nature and the same can be made applicable to any future innovations.
3) The last is the equivalence functional principle. It affords uniform treatment to transactions done online as that of transactions done offline.

All the states have tries to incorporate the UNCITRAL rules so as to bring uniformity in the laws.

This Model Law has been divided into two parts:

Part 1 deals with general provisions regarding e-commerce and Part 2 deals with specific provisions for e-commerce in certain areas.

Article 1 talks about information in the form of data messages in the framework of commercial activities.

Article 2 of this Act covers the definitions such as data message which uses the word ‘similar means to include any future developments.

Article 3 covers the interpretation techniques.

Article 4 covers variation in communication by agreement between both parties.

Article 5 information in electronic mode cannot be denied legal validity or enforcement.

Article 6 & 7 has removed the hindrance of the document to be in writing and handwritten signatures.

Article 8 talks about standard of reliability (for what reason the data was generated and other surrounding circumstances).

Some of the other general articles are Articles 9 to 15 which talks about evidentiary value granted to messages stored online, retention of information, formation of valid contract, acknowledgment in the form of receipt.

Some of the specific provisions are section 16 and section 17 which enlists carriage of goods and transport documents.

It is important to note that on the same grounds of model law, India had enacted The Information Technology Act, 2000. (Garg Ananya, 2020, p.l).

Check your progress 4: *Spend 3 Min*

Why was the UNCITRAL 1996 adopted?

4.7 Regulation of Cyberspace Content: Global Scenario

4.7.1: UNITED STATES

The exponential growth in the usage of online services in the United States in the late 1980s and early 1990s led to demands for its operations to be regulated.

Communications Decency Act 1996 (CDA)

The Section 502 of the CDA amended sections 223(a) and (d) of Title 47 of the United States Code ('USC'). It prohibits the making and transmission of obscene or 'indecent' material to a minor by means of a telecommunications device, and the use of an interactive computer service to send or display 'patently offensive' material to minors. The provisions also prohibited a person from knowingly permitting a telecommunications facility under that person's control to be used to commit these offences. However Supreme Court in American Civil Liberties Union v, Janet Reno, Attorney General of the United States; American Library Association, Inc. v, United States Department of Justice (the 'CDA Case', 1997) declared unconstitutional the above two statutory provisions as a violation of both freedom of speech and personal privacy.

COPPA

In 1998 US Congress enacted Children Online Privacy Protection Act (COPPA) which necessitated the federal trade commission to release and implement regulations concerning children's online privacy.

The Rule applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13, websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. The implementation of the Act was prohibited in the case of Aschcroft vs American Civil Liberties Union (2004) as it was likely to fail the "strict scrutiny" test due to the fact that it was not closely customized i.e., it prohibited online publishers from publishing some stuff that adults had a right to gain access to and since it did not utilize the minimum restrictive means feasible to safeguard children. **(Federal Trade Commission, p.1**)

CIPA

In 2000, Children Internet Protection Act (CIPA) was passed. This Act requires the schools and libraries to install filters on computers used by minors and adults.

Other Related Legislation

Uniform Electronic Transactions Act, 1999 (UETA) - to remove barriers to electronic commerce by validating and electronic records and signatures. However, the substantive rules of contract remain

unaffected by it. This Act only operates in some specific sorts of transactions and merely when the parties have approved to perform the transaction by electronic means. **(Sandra Norman-Eady, 2000, p.1)**

Uniform Computer Information Transaction Act, 2000 (UCITA)

According to UCITA, for a transaction to be 'Computer Information Transaction', the main focus of the transaction must be acquiring the computer information, access to it, or its use and not a mere incident of another transaction. The act applies to contracts for the development or creation of computer information, such as software development contracts and contracts to create a computer database. This Act does not apply to many cases in which one person provides information to another person for another transaction such as making an employment or loan application. The state of Maryland was the first state in which UCITA became effective. (**FindLaw Attorney Writers, 2017, p.1**).

The **Gramm-Leach-Bliley Act** (**GLB Act** or **GLBA**) or Financial Modernization Act of 1999. It is a United States federal law that calls for financial institutions to clarify how they share and keep their customers confidential information private. (**Federal Trade Commission, p.1**).

The **Health Insurance Portability and Accountability Act of 1996** (**HIPAA**) is a federal law that necessitated the formation of national standards to protect the patient's sensitive health information from being revealed without the permission from the patient or without the knowledge of the patient. **(Public Health Professionals Gateway, 2018, p.1)**

The **Fair Credit Reporting Act, 1970** was the first federal law to regulate the use of personal information by private businesses. **(Federal Trade Commission, p.1)**

The other cyber security laws to strengthen the domain in the US:

1. **Consumer Privacy Protection Act, 2017** aims at assuring the safety of personal information of users, to circumvent identity theft, to inform its citizens and organizations concerning security violations and to put a stop to the mishandling of sensitive user information. **(Gov track, 2017, p.1**)
2. **Cybersecurity Information Sharing Act (CISA)** is a proposed legislation that will permit United States government agencies and non-government agencies to dole out information with each other as they examine and scrutinize cyberattacks. (**Thomas F. Duffy, Chair, 2016, p.1)**
3. **Cybersecurity Enhancement Act of 2014** was signed into law on December 18, 2014. It provides an ongoing, voluntary public-private partnership to develop, enhance and upgrade and develop cybersecurity and boost cybersecurity research and development, workforce development and education and public awareness and preparedness. **(govinfo, p.1**)

4.7.2 European Union

The approach of a large majority of (perhaps all) European Union Member States in dealing with illegal and harmful content on the Internet appears to be in accord with the1996 recommendations of the European Commission advocating the use of filtering software and rating systems, and an encouragement of self-regulation of access providers. In these countries, laws regarding material that is illegal offline, such as child pornography and racist material, also apply to Internet content. With regard to material unsuitable for children, the EU Safer Internet Action Plan covering the period 1999-2002 has a budget of 25 million euro and has three main action lines;

- Creating a safer environment through promotion of hotlines, encouragement of self-regulation and codes of conduct,
- Developing filtering and rating systems, facilitation of international agreement on rating systems,
- Awareness: Making parents, teachers and children aware of the potential of the Internet and its drawbacks, overall co-ordination and exchange of experience.

The word 'cybersecurity', from the viewpoint of European Union, involves a blend of cyber resilience, cybercrime, cyber defence, (strictly) cybersecurity and global cyberspace concerns. It is noteworthy that while the two EU Cybersecurity approaches pursued the adoption of various legislative measures regarding cybersecurity, they put forward policy objectives which later resulted in legislation, namely the *Network and Information Security Directive* and the *Cybersecurity Act* (came into force on 27th June 2019.) which further sheds light on the job and order of the European Union Agency for Network and Information Security (ENISA). Building on this observation, it is proposed that the cybersecurity area recuperates itself by both law and policy measures. Policy measures from various policy areas eventually led to changes and adjustments in various EU legal frameworks and *vice versa*.

"*The EU General Data Protection Regulation (GDPR),* which governs how personal data of individuals in the EU may be processed and transferred, went into effect on May 25, 2018. GDPR is a comprehensive privacy legislation that applies across sectors and to companies of all sizes. It replaces the Data Protection Directive 1995/46. The overall objectives of the measures are the same – laying down the rules for the protection of personal data and for the movement of data". **(https://www.trade.gov/).**

4.7.3 UNITED KINGDOM

In September 1996, UK Government issued R3 Safety-Net action plan (now Internet Watch Foundation, IWF), developed by UK ISP trade associations and where it is agreed by Government involve industry for establishment of complaints hotline and related take-down procedures for illegal Internet content, primarily child pornography. In February 2002, the IWF announced that it would henceforth also deal with "criminally racist content".

Related Legislation in UK

1) The Computer Misuse Act, 1990 is an" Act to make provision for securing computer material against unauthorised access or modification; and for connected purpose" **. (legislation.gov.uk).**
2) Electronic Communications Act, 2000 to facilitate the use of electronic communications and electronic data storage.
3) Data Protection Act 2018 (DPA 2018) superseded Data Protection Act, 1998 and supplements the EU General Data Protection Regulation (GDPR). The act makes "provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes." (legislation.gov.uk))

National Cyber Security Centre (NCSC), UK – In 2016, CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure were merged to form National Cyber Security Centre. It provides a single point of contact

for SMEs, larger organisations, government agencies, the general public and departments and also works in collaboration with other law enforcement, defence, the UK's intelligence and security agencies and international partners. (**NCSC.GOV.UK**)

4.8 REGULATION OF CYBERSPACE CONTENT IN INDIA

In India, Information Technology Act, 2000 is the legislation which covers the domain of cyber law. The main objective of the Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as e-commerce, which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies.

Electronic Signatures [Chapter II]

Any subscriber (i.e., a person in whose name the Digital Signature Certificate is issued) may authenticate electronic record by affixing his Digital Signature. Electronic record means data record or data generated image or sound, stored, received or sent in an electronic form or microfilm or computer-generated microfiche.

Electronic Governance [Chapter III]

Where any law provides submission of information in writing or in the typewritten or printed form, it will be sufficient compliance of law, if the same is sent in an electronic form. Further, if any statute provides for affixation of signature in any document, the same can be done by means of Digital Signature.

Similarly, the filing of any form, application or any other documents with the Government Authorities and issue or grant of any licence, permit, sanction or approval and any
receipt acknowledging payment can be done by the Government offices by means of electronic form. Retention of documents, records, or information as provided in any law, can be done by maintaining electronic records. Any rule, regulation, order, by-law or notification can be published in the Official Gazette or Electronic Gazette.

However, no Ministry or Department of Central Government or the state Government or any Authority established under any law can be insisted upon acceptance of a document only in the form of electronic record.

Regulation of Certifying Authorities [Chapter IV]

The Central Government may appoint a Controller of Certifying Authority who shall exercise supervision over the activities of Certifying Authorities.

Digital Signature Certificate [Chapter VII]

Any person may make an application to the Certifying Authority for issue of Digital Signature Certificate. The Certifying Authority while issuing such certificate shall certify that it has complied with the provisions of the Act.

Penalties and Adjudication [Chapter IX]

If any person without the permission of the owner, accesses the owner's computer, computer system or computer net-work or downloads copies or any extract or introduces any computer virus or damages computer, computer system or computer net work data etc. he/ she shall be liable to pay damage by way of compensation not exceeding Rupees One Crore to the person so effected.

The Appellate Tribunal [Chapter X]

The section 48 of IT Act provides 'that The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997 shall, on and from the commencement of Part XIV of Chapter VI of the Finance Act, 2017, be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act. However, the Central Government shall specify, by notification, the matters and places in relation to which the Appellate Tribunal, may exercise jurisdiction'.

Under the act, the Central Government has the power to establish the Cyber Regulations Appellate Tribunal having power to entertain the cases of any person aggrieved by the Order made by the Controller of Certifying Authority or the Adjudicating Officer.

Offences [Chapter XI]

Tampering with computer source documents or hacking with computer system entails punishment with imprisonment up to three years or with fine up to Rs. 2 lakhs or with both.

Publishing of information, which is obscene, in electronic form, shall be punishable with imprisonment up to five years or with fine up to Rs. 10 lakh and for second conviction with imprisonment up to ten years and with fine up to Rs. 2 lakhs.

The Information Technology Act, 2000 was amended in 2015 wherein the Supreme Court in the case of Shreya Singhal v. Union of India had struck Section 66A of Information Technology Act, 2000 as it violates the freedom of speech and expression provided under Article 19(1)(a) of the Constitution of India.

Check your progress 5: *Spend 3 Min*

List the specific legislation in different countries to regulate cyber space.

4.9 INTERNATIONAL INITIATIVES FOR REGULATION OF CYBERSPACE

Today there is a need for an international framework of principles, guidelines and rules for global communications for the twenty-first century. In July 1997, the German Government hosted an International Conference in Bonn on the topic 'Global Information Networks', in cooperation with the

European Commission that resulted in the adoption of the 'Bonn Declaration' of the Ministers as well as declarations by industry and user participants. The Bonn Declaration pointed in the direction of:

1) using current national legal frameworks for the enforcement of criminal law provisions where appropriate in respect of on-line crime;

2) development by industry of common principles for schemes of self-regulation regarding content of on-line services; and

3) establishment of national hotlines for complaints regarding on-line content and for some appropriate interconnection and interaction between national hotlines.

Martin Bangemanns, EC Commissioner in her speech of 8 September 1997 to the International Telecommunications Union in Geneva has pointed out that there is a need for an international charter for global communications, and in particular governing activities carried out over the Internet that could provide a suitable framework covering such issues as the legal recognition of digital signatures, encryption, privacy, protection against illegal and harmful content, customs and data protection. The tools for achieving these objectives would include mutual recognition, self-regulation and, if needed, regulation.

In 29 June 1998, on invitation by Martin Bangemann, business leaders from around the world participated in a discussion on global communication issues, with the objective to explore the need for strengthened international coordination which resulted in the formation of Global Business Dialogue and it was resolved that wherever possible, it should avoid legislation, and concentrate on market-led, industry- driven, self-regulatory models and any regulation should ensure competition. It should focus on a well-defined list of issues on which quick progress can be made with the close cooperation of business, consumer groups and governments of all countries who wants to participate and work on these issues should be industry-led and coordinated with relevant international bodies. Two organizations closely involved in this process were the Transatlantic Business Dialogue and the US-Japan Business Council. Attendance at the first meeting of the GBD's Business Steering Committee took place in New York on 14 January 1999 and consisted largely of representations of major corporations from United States, Europe and Japan. However, the issue of Internet content was not considered amendable to relatively fast solutions by the GBD and so Internet content is not receiving immediate attention from this Group.

In 27 February 1999, the first meeting of the International Network of Experts on Self-Regulation for Responsibility and Control on the Internet was held at New York. This network was brought together by the Bertelsmann Foundation, a charitable foundation which owns the controlling interest in Bertelsmann Corporation, the German media and publications enterprise, as a part of its advocacy of self-regulatory solutions to the problems of Internet content. The three regulatory agencies represented at the meeting were the Australian Broadcasting Authority, the Canadian Radio Telecommunications Commission (by Mr. Ted Woodhead) and the Singapore Broadcasting Authority (by Ms. Ling Pek Ling); all of which are actively dealing with the issues of self-regulation of harmful content on the Internet.

The above study reflects initial approaches and legal policies in the world in context of regulation of cyberspace and International efforts to deal with it but due to democratic and challenging nature of

cyberspace the efforts on the part of various international organization is required to deal with the cybersecurity and share information so that harmonious regional efforts can be taken to regulate the cyberspace keeping in pace with technology. The role of few of the organizations have been discussed below:

4.9.1 Organization for Economic Cooperation and Development (OECD)

The OECD an international organization working in the area of data privacy and information security, established an ad hoc process of meetings (the first was on 1-2 July 1997 and second on 22 October 1997) on approaches being taken in major industrial countries for the regulation of content conduct on the Internet. The meeting acknowledged the primary role of the private sector in regulating the Internet. However, at the joint OECD/Business and Industry Advisory Committee forum held on 25 March 1998 in Paris, the OECD resolved to do no further work in this area. On 19 April 2006, OECD task force on spam has recommended that Governments and industry should step up their coordination to combat the global problem of spam. It calls on governments to establish clear national anti-spam policies and give enforcement authorities more power and resources. Co-ordination and co-operation between public and private sectors are critical, the report notes.

4.9.2 UNESCO

The United Nations Educational, Scientific and Cultural Organization (UNESCO) was founded on 16 November 1945. At the 29th UNESCO General Conference held in Paris from 21 October to 12 November 1997 the Director-General of UNESCO made a preliminary report on the feasibility of an international instrument on the establishment of a legal framework relating to cyberspace. It recommended the preservation of a balanced use of language on cyberspace, which represented the concern of non-Anglophone countries at the domination of English as the language of the Internet. Today, UNESCO functions as a laboratory of ideas and a standard-setter to forge universal agreements on emerging ethnical issues: the organization also serves as a clearing house – for the dissemination and sharing of information and knowledge – while helping Member States to build their human and institutional capacities in diverse fields.

4.9.3 Cyberbrics- This project has a threefold purpose. Firstly, to plot the prevailing protocols; to recognize finest procedures or ways and build policy propositions in the arena of cybersecurity governance (including personal data regulation), Internet access policy and tactics for the digitisation of public supervision in the BRICS (Brazil, Russia, India, China and South Africa).The focus areas are: data protection, consumer protection, cybercrime, protection of public order and lastly cyber defense.This endeavour or venture is held by Fundação Getulio Vargas (FGV) Law School and expounded in collaboration with the Higher School of Economics, in Moscow, Russia; the Centre for Internet and Society, New Delhi, India; the Fudan University, Shanghai, and the Hong Kong University, China; and the University of Cape Town, Cape Town, South Africa. (**Cyberbrics, p.1**)

Check your progress 6: *Spend 3 Min*

What are the international initiatives for regulation of cyberspace?

Please answer the following to check your progress.

Check your progress 7: Spend 3 Min.

State whether the following statements are true or false:

a) In Australia, government has mandated blocking of access to content deemed unsuitable for adults.

.....

b) In Korea, the government has no system of Internet content grading.

.....

c) Australian Broadcasting Authority and Singapore Broadcasting Authority are the only two regulatory agencies in the meeting of International Network of Experts (Feb, 1999).

Let us now summarize the points covered in this unit.

4.10 SUMMARY

- There has been rapid increase in use of internet for various types of commercial transactions and consumer services.
- For the safe carriage and conduct of Cyberspace, regulation ought to be identified as appropriate and necessary.
- The necessity arises due to the expansion of economic and creative interaction which in term led to disputes involving acquisition, use, possession, processing and communication of information.
- The use of internet for obscene, indecent and pornographic content, rumor mongering, viruses, cyber crime, possibility of invasion of privacy of individuals, all this emphasized the need for cyberspace regulation.
- Legal policies in various countries like USA, UK, European Union, and New Zealand show that in the context of regulation of Cyberspace more emphasis is on self regulation through use of filtering/blocking technologies.
- There is need for coordinated international guidelines and principles to regulate cyberspace.
- International organizations such as OECD, UNESCO, Cyber BRICS can play an important role in framing international regulatory framework for internet.

4.11 ANSWERS /SOLUTIONS

Check your progress:

1. Cyberspace is susceptible to a variety of threats and needs to be immediately addressed. However, the cyber society is more focused on upgrading the technology rather focusing on taking clear measures to stabilize this domain despite being aware of the emerging threats. Hence, it is crucial to mend the existing state the cyber space is in. The ease of accessing materials which are obscene and have indecent content should be looked into, the increasing business transaction from tangible assets to intangible assets needs attention due to both regulatory and jurisdictional issues, data protection and data privacy laws should be stringent so that the users are confident as to accessing the internet.
2. Privatization: The state can use a private body to achieve those goals which it could not get directly and then implement that body's decision through mandatory technological arrangements. Propertization: According to him, first of all an attempt is to be made to extend and then protect intellectual property rights online. This will produce many technical methods of enforcement.
   Technological Controls: The system is to be designed so as to hardware in desired regulatory features.
   Blocking software or Internet contents grading system are other forms of regulations based on technology.

3. In recent times, the internet design has excluded government control for regulation of cyberspace, the government role has turned to be very minimal. But some argue that government intervention is necessary for regulating this domain. Some of the countries like UK, Canada, New Zealand and a considerable number of Western European countries have adopted the approach of end-user voluntary use of filtering/blocking technologies.

4. It was adopted by the UN Commission on International Trade Law in 1996 in furtherance of its mandate to promote the harmonization and unification of international trade law, so as to remove unnecessary obstacles to international trade caused by inadequacies and divergences in the law affecting trade.

5. In the United States, Communication Decency Act, 1996, Internet Online Summit held in 1997, COPPA, 1998 which was regarding children's online privacy, CIPA, 2000 which requires the schools and libraries to install filters on computers used by minors and other legislations like the Uniform Electronic Transactions Act, 1999 to remove barriers regarding electronic signatures, Uniform Computer Information Transaction Act, 2000 and many other legislations. In the United Kingdom, Computer Misuse Act, 1990 which had introduced three concepts regarding unauthorized access to facilitate an offence by modification. Organisations like CERT-UK and Centre for Protection of National Infrastructure was established to handle cyber security. In India, the legislations are The Information Technology Act, 2000 and Indian Penal Code which deals with cyber offences and penalties.

6. Organisation for Economic Cooperation and Development has been playing an important role in the area of privacy, security, protecting children online and data governance; UNESCO focuses on the sum of processes and technologies used for free flow of information in the public domain; The CYBERBRICS project which has a triple aim of mapping existing regulations, identifying best practices and developing policy suggestions in the areas of cybersecurity governance,

Internet access policy and strategies for the digitalisation of public administrations in the 4 countries.

7. (a)True, (b) False & (c) False

4.12 REFERENCES/FURTHER READINGS

- Computer Misuse Act 1990. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/introduction
- CyberBrics. Retrieved from https://cyberbrics.info/
- Data Protection Act 2018. Retrieved from https://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted
- Dr. Dan L. Burk (1997). Jurisdiction in a Word without Borders. *Virginia Journal of Law and Technology university of Virginia.* Retrieved on 23 Nov. 2006 from <http:/ vjolt.student.virginia.edu>.
- Electronic Frontiers Australia (2002). Internet Censorship: Law and Policy around the world. *Electronic Frontiers Australia (EFA*). Retrieved on 2 Dec.2006 from <http://www.efa.org.au/>.
- *European Union - Data Privacy and Protection.* Retrieved from https://www.trade.gov/european-union-data-privacy-and-protection.Federal Trade Commission. *Fair Credit Reporting Act*. Retrieved from https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act
- Federal Trade Commission. *Gramm Leach Bliley Act*. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- Federal Trade Commission. *COPPA*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions 0#A.%20General%20Questions
- Find Law Attorney Writers (2017). Maryland adopts uniform computer information transactions act. Retrieved from https://corporate.findlaw.com/business-operations/
- Gareth Grainger (1998). Freedom of Expression and regulation of Information in Cyberspace: Issues concerning potential information cooperation principles for cyberspace. speech given at UNESCO INTERNATIONAL CONGRESS, INFO Ethics '98, Monte Carlo, Monac. 1 Sept. 1998.
- Garg Ananya (2020). Model Law on Electronic Commerce. Retrieved from https://blog.ipleaders.in/model-law-on-electronic-commerce/
- Govinfo (n.d). Cybersecurity Enhancement Act of 2014. Retrieved from https://www.govinfo.gov/app/details/PLAW-113publ274
- Govtrack (n.d). Consumer Privacy Protection Act of 2017. Retrieved from https://www.govtrack.us/congress/bills/115/s2124

- History of the NCSC. Retrieved from https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.
- James Boyle. In a Non-Delegation Doctrine for the Digital Age. Duke L.J. 5.50.
- Joshi Divij (nd). Comparison of legal and regulatory approaches to cyber security in India and the United Kingdom. The centre for internet and society. Retrieved from https://cis-india.org/
- Lawrence Lessing (1991). Commentaries – The Law of the Horse: what cyberspace might teach. *Harvard Law Review.* 113:501. Retrieved from <http:// www.lessing.org/ control/articles/works/finalhls.pdf>.
- Lawrence Lessing (1998). The Laws of Cyberspace. essay presented at – Taiwan Net '98 Conference in Taipei. Retrieved 24. Nov. 2006 from <http://www.lessing.org/ content/articles/works/laws_cyberspacepath>.
- Lawrence Lessing (1999). Code and Other Laws of Cyberspace. 85-99.
- Martin Bangemann's (1997). New World Order for Global Communications – The Need for an International Charter. Speech given at International Telecommunications Union, Geneva.8 Sept. 1997.
- OECD (April 2006). Anti-Spam Toolkit of recommended policies and measures. *OECD Task force on Spam*. Retrieved on 30 Dec. 2006 from <http://www.oecd-antispam-org>.
- Public health professionals gateway (2108). Health Insurance Portability and Accountability Act of 1996. Centres for disease control and prevention. Retrieved from https://www.cdc.gov/phlp/publications/topic/hipaa.html
- Sandra Norman (2000). Uniform Electronic Transaction Act. Retrieved from https://www.cga.ct.gov/2000/rpt/2000-R-1076.htm
- Thomas F. Duffy (2016). Cybersecurity Information Sharing Act of 2015. Retrieved from https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/

UNIT 5 CYBER CRIMES

Structure

5.0 INTRODUCTION

The purpose of the Information Technology Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information. It also aims at facilitating electronic filing of documents with the Government agencies.

This law is based on the UN General Assembly resolution A/RES/51/162, dated the 30th January, 1997 the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL). Need was felt for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

The act has undergone several amendments since its enactment in the year 2000. The most significant amendment is of 2008 which tried to address a number of issues keeping in view the technological development which facilitated the commission of certain offences which had a greater impact on the society. In this unit the wrongful acts covered in the act will be discussed. Some wrongful acts are civil wrong for which the aggrieved party is entitled to penalty or compensation. Some acts are treated as crime for which punishment is provided. The unit will also touch upon the issues involved in the investigation of these offences. The investigation of these offences requires scientific knowledge which is called Cyber Forensics.

5.1 OBJECTIVES

After reading this unit you should be able to:

1. Describe the acts for which penalties and compensation are provided. Also discuss when these acts become an offence.
2. Discuss the offences for which punishment is provided.
3. Examine the jurisdictional issues involved in the investigation and punishment of the cybercrimes.
4. Discuss the challenges faced by investigation agencies in investigation of cyber crimes, Penalties, compensation and adjudication. .

5.2 CYBER CRIME AND ITS CLASSIFICATION

Cybercrime is defined as crimes committed on the internet using the computer as a tool to target the victim for the execution of the desired crime. Though it is difficult to determine that where the particular cyber crime took place because it can harm its victim even sitting at a far distance. As stated above from the year 1997 to 2008 tremendous changes took place which helps the judicial system to determine the specific kind of cyber crime. However, all cybercrimes involved both the computer and the person behind it as victims, it just depends on which of the two is the main target.

Example 1 – Hacking involves attacking the computer's information and other resources.
Example 2 – Stalking involves attacking the personal space of an individual.

- Cyber crimes are quite different from traditional crimes as they are often harder to detect, investigate and prosecute and because of that cyber crimes cause greater damage to society than traditional crimes. Cyber crime also includes traditional crimes conducted through the internet or any other computer technology. For example; defamation, forgery, identity theft, terrorism, cyber-stalking, hacking, software piracy, web jacking and bullying are considered to be cyber crimes when traditional crimes are committed through the use of a computer and the internet.

The other difference between these two crimes is based on the evidence of the offences. In the traditional crimes the criminals usually leave any proof of that crime like fingerprints or other physical proof. But in the cyber crimes cyber criminals commit their crimes through the internet and there are very less chances of leaving any physical proof.

However, the cyber crimes are broadly classified into different groups:

1 Crime against the individuals – Harassment, cyber-stalking, deformation, indecent exposure, cheating, email spoofing, fraud, etc.

2 Crime against property – Transmitting virus, net-trespass, unauthorized control over computer system, internet thefts, infringement of intellectual property,etc.

3 Crime against organization – Cyber terrorism within government organization, possession of unauthorized information, distribution of pirate software, etc.

4 Crime against society – Child pornography, financial crimes, sale of unlawful articles, trafficking, forgery of records, gambling, etc.

☞ **Check your Progress 1:**

1. Distinguish between cyber crime and traditional crime.

.....

.....

.....

.....

5.3 PENALTY AND COMPENSATION

Section 43 to 45 of Information Technology Act, 2000 provides for the instances where the wrong doer is liable to pay damages by way of compensation to the effected party.

Section 66 of Information Technology Act, 2000 however provides that if any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Section 43 of Information Technology Act, 2000 provides that any person who without permission of the owner or any other person who is in charge of a computer, computer system or computer network commits the following acts shall be liable to pay damages:

(a) Accesses or secures access;
(b) downloads, copies or extracts any data, computer data base or information;
(c) introduces or causes to be introduced any computer contaminant or computer virus;
Explanation to this section provides:
"Computer contaminant‖ means any set of computer instructions that are designed–
(a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system, or computer network;
(iii) ―computer virus‖ means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;"
(d) damages or causes to be damaged data, computer data base or any other programs;
Explanation

(iv) of this section provides, " damage‖ means to destroy, alter, delete, add, modify or rearrange any computer resource by any means."
(e) disrupts or causes disruption;
(f) denies or causes the denial of access to any person authorised to access by any means;
(g) provides any assistance to any person to facilitate access in contravention of the provisions of this Act, rules or regulations made there under;
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating;
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]
[(v) ―computer source code‖ means the listing of program, computer commands, design and
layout and program analysis of computer resource in any form.]

Section 43A of Information Technology Act, 2000 provides for the liability for Compensation of a body corporate for failure to protect data.
Explanation to this section defines a body corporate as: "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

The explanation also defines reasonable security practices and procedures as, "security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

Section 44 of Information Technology Act, 2000 provides for penalty for failure to furnish information, return, etc
"If any person who is required under this Act or any rules or regulations made there under to–
(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(b) file any return or furnish any information, books or other documents within the time specified
therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues."

Section 45 of Information Technology Act, 2000 provides for the residuary penalty. Contravention of any rules or regulations made under this Act, for the

contravention of which no penalty has been separately provided. The maximum penalty in such cases is 25000 rupees.

5.3.1 Adjudication

Section 46 provides for the adjudication of disputes for awarding compensation. It authorizes the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry. This officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore. a reasonable opportunity for making representation in the matter and on such inquiry must be given.

Where it accedes 05 (five) crore,The jurisdiction shall vest with the competent civil court:

1. All proceedings before adjudicating officer shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code, 1860;
2. It shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973;
3. It shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.

No person shall be eligible to be appointed as an adjudicating officer if he does not possesses such experience in the field of Information Technology and legal or judicial experience which is explicitly prescribed by the Central Government.

5.3.2 Appellate Tribunal–

An appeal tribunal is a special court or committee that is formed to reconsider a decision made by another court or committee.

Section 48 provides that from coming into force of the Finance Act, 2017 Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997), shall be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act.

Section 57 provides the procedure for appeal. Any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Appellate Tribunal having jurisdiction in the matter. However no appeal shall lie to the Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. Every appeal shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

The appeal shall be dealt with as expeditiously as possible and endeavor shall be made to dispose of the appeal finally within six months from the date of receipt of the appeal.

Section 58 provides that Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, it shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:–
(a) Summoning and enforcing the attendance of any person and examining him on oath;
(b) Requiring the discovery and production of documents or other electronic records;
(c) Receiving evidence on affidavits;
(d) Issuing commissions for the examination of witnesses or documents;
(e) Reviewing its decisions;
(f) Dismissing an application for default or deciding it ex parte;
(g) Any other matter which may be prescribed.

Section 62 provides for the appeal to high court. Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order on any question of fact or law arising out of such order:
Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

☞ **Check your progress 2:**

1. Describe in brief the procedure for adjudication under the Information Technology Act, 2000

.....

.....

.....

.....

5.4 OFFENCES

Following acts are considered as offences under the act:

Section 65 provides for tampering, concealing, destroying , or altering any computer source document intentionally. Penalty is up to Rs.2,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 66 provides for dishonestly, or fraudulently doing any act as referred in Section 43. Penalty is up to Rs.5,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 66A has been struck down by Supreme Court's Order dated 24th March, 2015 in the landmark precedent of "*Shreya Singhal vs. Union of India*", AIR 2015 SC.1523.25. The court found it as violation of the Freedom of Speech and Expression guaranteed under the Constitution of India.

Section 66B provides for dishonestly, or fraudulently receiving or retaining any stolen computer resource or communication device. Penalty is up to Rs.1,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 411 of the IPC, 1860 provides punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 years,

Section 66C provides for dishonestly, or fraudulently making use of Electronic Signature, Password or any other Unique Identification Feature of any other person. Penalty is up to Rs.1,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 66D provides for dishonestly, or fraudulently by means of any communication device or computer resource cheating by personating. Penalty up to Rs.1,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 419 of the IPC, 1860 provides punishment for 'cheating by personating' and provides that any person who cheats by personating shall be punished with imprisonment of either description for a term which may extend to 03 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personating' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

Section 420 of the IPC, 1860 provides for any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 07 (seven) years, and shall also be liable to fine.

Section 66E of Information Technology Act, 2000 provides for intentionally capturing, publishing, or transmitting image of private area of any person without consent. Penalty is up to Rs.2,00,000/-, or Imprisonment up to 03 (three) years, or both.'

Section 66F provides for doing any act electronically, or with use of computer with intent to threaten unity, integrity, security, or sovereignty of India. Punishment is Imprisonment for Life.

Section 121 of the IPC, 1860 provides for waging, or attempting to wage war, or abetting waging of war, against the Government of India does cover this offence partially.

Section 67 provides for publishing, or transmitting in electronic form any material which appeals to prurient interest, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see, or hear matter contained in it. Penalty is up to Rs.5,00,000/-, or Imprisonment up to 03 (three) years, or both, And in the event of second or subsequent conviction, shall be liable to pay penalty up to Rs.10,00,000/-, or Imprisonment up to 05 (five) years, or both.

Section 67A provides for publishing, or transmitting in electronic form any material which contains sexually explicit act, or conduct. Penalty is up to Rs.10,00,000/-, or Imprisonment up to 05 (five) years, or both, And in the event of second or subsequent conviction,

this section however provides that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–
(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest
of science, literature, art or learning or other objects of general concern; or
(ii) which is kept or used for bona fide heritage or religious purposes.

The provisions of sections 292 and 294 of the IPC, 1860 would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC, 1860 provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 02 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 05 years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 294 of the IPC, 1860 provides for any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 03 months, or with fine, or with both.

Section 68 of IT Act, 2000 provides for the Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under and if any person who intentionally or knowingly fails to comply with the order, shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 (two) years, or both.

Section 69 provides that where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may with reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource, Any person who fails to comply with the order, then he shall be liable to Imprisonment of 07 (seven) years, along with the fine (amount of fine is not specified in the act).

Section 70authorises the Government to declare by notification in the Official Gazette, any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Any person who fails to comply with the notification, shall be liable to Imprisonment of 10 (ten) years, along with the fine.

Section 71 provides that whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any License or Electronic Signature Certificate, as the case may be, shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 (two) years, or both.

Section 72 provides that if any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person, shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 years, or both.

Section 72A provides that if any person who has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, shall be liable to pay penalty up to Rs.5,00,000/-, or Imprisonment up to 03 years, or both.

Section 73 provides that if any person publishes a Electronic Signature Certificate, or make it available to any other person with the knowledge that
- Certifying Authority has not issued it, or
- Subscriber has not accepted it, or
- Certificate has been revoked or suspended shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 years, or both.

Section 74 provides that if any person knowingly creates, publishes, or otherwise makes available Electronic Signature Certificate for any fraudulent

or unlawful purpose, shall be liable to pay penalty upto Rs.1,00,000/-, or Imprisonment up to 02 (two) years, or both.

☞ **Check your progress 3:**

1. In which Supreme Court case and on what ground section 66A of Information Technology Act, 2000 was struck down.

.....

.....

.....

.....

5.4.1 Liability of Network Service Providers

A 'network service provider' means any person who provides access to information service in electronic form. For example: Internet service provider, cellular mobile services, customer access services, mobile satellite services etc. It essentially performs two tasks-to provide access to the network and to act as intermediary between an originator and addressee with respect to any particular electronic message.

Section 79 provides certain exemptions from liabilities to intermediaries i.e. internet service providers etc. An intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. This exemption shall apply if–
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
(b) the intermediary does not–
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;
(c) the intermediary observes due diligence while discharging his duties under this Act and also
observes such other guidelines as the Central Government may prescribe in this behalf.

The above exemption shall not apply if–
(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its
agency that any information, data or communication link residing in or connected to a computer
resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

☞Check Your Progress 4:

1. What are the grounds which exempt the network service provider from liability?

.....

.....

.....

.....

5.4.2 Investigation

For the purpose of conducting cyber-crime investigation, essential special skills and technical tools are required without which the investigation is next to impossible. After commencement of the Information Technology Act, 2000, some provisions of Criminal Procedure Code, 1973 and the Evidence Act, 1872 have been duly amended. Along with these, certain new rules and regulations had been enforced by the Indian legislative system to meet the need of cyber-crime investigation.

Section 75 deal with the issue of jurisdiction with respect to cyber crimes. As we know, cyber crime knows no boundary. A person sitting in one country can commit offences having its consequences in another country. Section 75 provides that if any person have committed an offence, or contravention committed outside India, and if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India, then the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Section 76 provides that any computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto, in respect of which any provision of this Act, rules, orders, or regulations made there under has been, or is being contravened, shall be liable to confiscation. However, if it is proved that such resources were not used in committing fraud then only person in default will be arrested.

Section 77 provides that compensation, penalties or confiscation shall not interfere with other punishment.

Section 77A deals with compounding of offences. A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding 03 (three) years has been provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

Section 77B provides that offences with three years imprisonment shall be bailable.

Section 78 deals with the power to investigate. It provides that a police officer not below the rank of inspector shall investigate any offence under this Act.

Section 80 deals with the power of police officer and other officers to enter, search etc. It provides that any police officer, not below the rank of a inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. Where any person is arrested by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

☞ **Check Your Progress 5:**

1. How the issue of jurisdiction of Indian courts with respect to offences committed outside India has been dealt with by the IT Act?

.....

.....

.....

.....

5.5 CYBER FORENSICS

Cyber forensics also known as computer forensics which is the application of investigation and analysis techniques to gather and store evidence from a particular computing system in a way that is appropriate for presentation in a court of law.

Section 79A authorizes Central Government to notify any department, body or agency of the Central Government or a State Government as an Examiner of electronic evidence for the purposes of providing expert opinion on electronic form evidence before any court or other authority.

"Cyber forensics is the process of acquisition, authentication, analysis and documentation of evidence retrieved from the systems or online used to commit the crime. The systems could be from computers, networks, digital media or storage devices that could contain valuable information for the investigators to examine. From online, it could be from e-commerce domains or other websites. In cyber forensics, file or data carving techniques are most

commonly used to extract digital evidence from the source, hard drive or online domain. Computer forensics is important not just because it does recover files hidden or deleted away from storage devices and systems but it can also tell forensics experts whether are there any suspicious activities going on or had the systems been tampered with. Computer forensics had helped solved the issue of recovering information from files where file system is unavailable or file system structure is corrupted. Files may be intentionally deleted or worse formatted to the interest of the suspect to conceal his actions. In today's modern era where technology plays a part in almost all the electronic devices, it is important to know when required, how a trained forensics specialist can perform up to expectation, in collecting and present his evidence findings to corresponding agencies.

Examinations of forensics evidence are normally held in forensics laboratories or clean rooms by computer forensics investigators. A good and knowledgeable forensics expert is best preferred to be in the process of examination, as it is always vital to perverse the integrity of the data and not destroy it. Many forensics experts have their own standards and procedures on how computer forensics examinations are conducted which can be a big issue. Having double standards could jeopardize the integrity, creditably and validity of the digital evidence which could result in serious implications along the way. Therefore, as early as 1991, suggestions were made to streamline and standardize the examination processes and protocols had been raised. The purpose was to smoothen out rough edges approach used in evidence finding. Eventually, all these led to the formation of International Organization on Computer Evidence and Scientific Working Group on Digital Evidence (SWGDE). It became a worldwide effort to help law enforcement agencies around the globe to work together more closely with regards to forensics examinations.

Digital forensics is a branch of forensic science which deals with recovery and investigation of digital or electronic data. This data can be from a computer system, mobile device, cloud service, and so on. Its various sub branches include computer forensics, network forensics, forensic data analysis, and mobile device forensics.

Cyber or computer forensics is the application of forensic science to collect, process, and interpret digital evidence to help in a criminal investigation and presenting digital evidence in a court of law. It is the branch of forensic science in which evidence is found in a computer or any other digital device and with increasing cybercrime, cyber forensics has now become crucial for public safety, national security, and law enforcement**.**

☞Check your progress 6:

1. What is Cyber Forensics?

.....

.....

.....

.....

5.5.1 Cyber Forensic Investigation Tools

Cyber forensic techniques include:

1. Cross-driven analysis that correlates data from multiple hard drives.
2. Live analysis, which obtains data acquisitions before a PC is shut down.
3. Deleted file recovery.
4. Detecting data theft using Stochastic Forensics.
5. Concealing a file, message, image, or video within another file using Steganography.

Computer forensic investigations go through five major standard digital forensic phases:
1. Policy and procedure development,
2. Assessment,
3. Acquisition,
4. Examination, and
5. Reporting.

Digital evidence is so fragile, it can be easily damaged, modified or destroyed purposely. That is why most of the time, original evidence are often duplicated and analysis is carried out on the duplicated copy to prevent any mishap of damaging the original copy. Scope of digital evidence examination can be very broad, it can be either online or offline. Examples of them are credit card transactions, Internet communications history, hard drives and other storage devices.

Digital evidence is very critical to an investigation because the information on the evidence can tell the investigator what really happened and pieced together the whole picture. Forensics experts are looking for any form of metadata, suspicious content and other data residing in the hard drive. Every single click by the user on the computer was recorded by the system and a trained forensics expert can tell from one look what types of activity and desire the user was engaged in. better than anyone else. The recorded logs act like a behavioral database, documenting every single movement on the laptop used by anyone.

There are methods and techniques out there to aid fellow forensics experts to prevent digital evidence from being unintentionally tampered with. Experts can utilize method such as Imaging and Write-block. Imaging is equivalent to ghosting a backup copy of the whole computer hard drive (evidence) into a soft copy. So investigators work on the ghosted copy of the hard drive and the original hard drive is kept one side. In any case, if the ghosted copy is corrupted; investigators can pull out the original hard drive and create another copy to work on. Write-block is another good way to prevent original evidence being altered. The evidence media is connected with a special machine that can prevent any attempt to overwrite the data on the device. Thus, the evidence on the hard drive cannot be altered as any attempt to write on the media had been blocked by the special machine.

The reason behind preservation of digital evidence is simple. When submitting digital evidence for documentations or legal purposes in any court or legal department, legitimate proof is required to show correct findings on the

investigation. It had to show the same as the exhibit seized at the crime scene. This phenomenon is also commonly known as chain of custody. For example, in a cyber-forensics crime environment, such exhibits would be media storage devices, a copy of digital evidence from the hard disk seized and so on. Chain of custody basically is a map that clearly depicts the process of how digital evidence were processed; collected, analyzed and preserved in order to be presented as digital evidence in court. A chain of custody will also be needed to showcase whether the evidence is trustworthy or not. To meet all the requirements for chain of custody, three criteria are essential. Firstly, no alteration must be done to the evidence from the day of seizure. Secondly, a duplicate copy needed to be created and it had to be functional; not corrupted. Lastly, all evidence and media are secured. Able to provide this chain of custody is unbroken is an investigator primary tool in authenticating all the electronic evidence.

If the chain of custody is broken, digital evidence collected from the scene submitted to the court can be denied as the evidence might had been altered and might not tell the truth of the evidence. This is a prosecutor worst nightmare. In any situation, chain of custody is best followed to prove that evidence does not get contaminated and stayed in original state. However, there are occasions where collecting evidence without altering the data is not possible, especially when forensics tools were used. Such act will prove to be a serious implication to justify the evidence is intact and submission of such evidence will be challenged by the opposing team.

Locate Evidence once preserving the evidences is done, it's time to locate relevant evidence that can make a difference in the legal battle. The general first rule of thumb when locating the evidence is do not rush, as one is eager to get the investigation started, wants to find as many evidences as possible. However, the more one rushes the more mistakes the one is likely to make. Rushing into an investigation can have dire consequences, consequences like causing evidence to be lost prematurely or altered unintentionally.

Besides locating evidence, investigators must also maintain high integrity and reliability of the digital evidence, doing so, will minimize metadata being altered and destruction of important evidence. Digital evidence can be in any file format; email, notepad or video or it can have no file format due to the fact that it had been encrypted. Forensics experts need to browse through thousands of files in the computer system or network to spot and collect suspicious files. Forensics experts are trained and taught to focus on area of interests within the system. Examples of such areas are like Recycle bin, Windows Registry and Internet Temp Folder. Focusing on these areas saved tremendous hours of searching. These areas will tell the investigators what took had happened and who did it. To examine such a wide range of file types after taking consideration the area of interests. The process of examination gets whole lot tougher and tedious. Investigators will bring in tools to help facilitate them with locating and collecting of the evidence. Forensics experts often use tools like OS forensics, XYR tools, Quickstego or other sophisticated toolkits to aid them in the finding. All these tools will help investigators to decide whether they are looking at the correct areas or not and whether did they missed out anything important. Such equipment not only uncovers hidden or deleted files, it can also reveal the importance of the file whether it is relevant to the case or not.

☞ **Check your progress 7:**

1. What are the techniques used by forensics experts?

.....

.....

.....

.....

5.6 SUMMARY

In this unit we have discussed the penalties and offences provided under the Information Technology Act, 2000. Any type of unauthorized intrusion in the computer, computer system or network is prohibited and any person who does it is liable to pay compensation.

The penalties include: introducing viruses in the computer system, unauthorized download of copyrighted material, charging services in the name of others etc.

Offences covered in the act are mainly related to hacking, misrepresentation, identity theft, publishing obscene material, child pornography, unauthorized access to protected system etc.

Investigation of cyber crime is a big challenge. Cyber criminals are mainly educated and well versed in technology. Therefore investigation of cyber offences requires training in skills of cyber forensics.

5.7 SOLUTION/ANSWERS

1. **Cyber crime are those offences in which computer is used as tool or target or both in committing offences. The term includes the offences covered under the IT Act such as unauthorized access to a computer or introducing viruses etc and traditional crimes covered under the Indian Penal Code or other legislations such as forgery, defamation etc.**
2. **IT Act provides that for adjudication of penalty and compensation upto 5 crore rupees, there shall be the Adjudication officer. Against its decision, appeal can be filed before the Appellate Tribunal and second appeal to the High Court. Adjudicating Officer have the power of civil court for certain purposes. No appeal will lie where the order is based on the compromise between the parties. For amount acceding 5 crore rupees, the civil courts have the jurisdiction.**

3. "Shreya Singhal vs. Union of India" is the landmark judgment which struck down section 66A of Information Technology Act, 2000 on the

ground that it puts unreasonable restriction on the Freedom of Speech and Expression guaranteed by the Constitution of India.

4. An intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. This exemption shall apply if–
5. (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
   (b) the intermediary does not–
   (i) initiate the transmission,
   (ii) select the receiver of the transmission, and
   (iii) select or modify the information contained in the transmission;
   (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

6. Section 75 provides that if any person have committed an offence, or contravention outside India, andit involves a computer, computer system or computer network located in India, then the provisions of this Act shall apply also to such person irrespective of his nationality.

7. Cyber forensics also known as computer forensics which is the application of investigation and analysis techniques to gather and store evidence from a particular computing system in a way that is appropriate for presentation in a court of law.

8. The techniques used by forensics experts are as follows:
   Cross-driven analysis that correlates data from multiple hard drives.
   Live analysis, which obtains data acquisitions before a PC is shut down.
   Deleted file recovery.
   Detecting data theft using Stochastic Forensics.
   Concealing a file, message, image, or video within another file using Steganography.

5.8 REFERENCES

- UKEssays. (November 2018). What Is Cyber Forensic Information Technology Essay? Retrieved from https://www.ukessays.com/essays/information-technology/what-is-cyber-forensic-information-technology-essay.php?vref=1
- Vinod Joseph and Deeya Ray (Feb 2020). Cyber Crimes under the IPC and IT Act - An Uneasy Co-Existence. Retrieved fromhttps://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence.
- Information technology Act, 2000.
- Indiacode, Information Technology Act, 2000 available at https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&sectionId=13011&sectionno=2&orderno=2

UNIT 6 IPR ISSUES IN CYBER SPACE

Structure

6.0 INTRODUCTION

Management of Intellectual Property Rights in cyberspace is an important issue to combat property infringements in the virtual space ensuring security to the Intellectual Property Rights holders that they can control the use of their intellectual property and be protected from unauthorised or unlicensed use of literary work, trademarks, trade names, service marks, images, music or sound, piracy of software's. The Infringements in digital media may take different forms that include Copyright's violations, Deep Hyper linking, Framing, Meta-tags, spamming. The Trademark violation is the most crucial issue giving rise to Domain Name Disputes and cybersquatting, where the defendant/infringer intentionally gets the domain name registered that includes the trademarked words, company name, brand name etc. of the plaintiff company.

The traditional laws for protecting intellectual property have been also applicable to the infringements taking place in digital media. However, due to inherent nature of the internet, the relative anonymity afforded to the digital transactions , jurisdiction issues, the ease of copying and distribution of copies, several pertinent issues have emerged in recognizing various forms of online infringements and resolving conflicts of owner of the right holders, of authors, publishers, film producers, music creators and software developers exploring ways to make their products available online, while protecting their rights and recouping their investment.

One cannot deny that the Information Technology Act, 2000 has proven to be successful in setting down the framework of laws and regulation in cyber space and addresses numerous concerns related to the misuse of technology, but at the same time the particular Information Technology Act, 2000 suffers from some of the serious lacunae which all have not been primarily discussed, known as intellectual property issues. Further, Intellectual property is considered as an intangible asset therefore, there has to be specific penal provisions under Information Technology Act, 2000, as the infringement of the intellectual property is very easy in the cyberspace.

6.1 OBJECTIVES

After studying this unit learner will be able to:

- Discuss the basic concept and various forms of Intellectual Property Rights.
- Analyse the copyright issues in digital- medium, music and goods.
- Discuss the concept and issues of Linking, In-lining and Framing
- Discuss patent infringement through digital medium
- Describe Trademark issues and Domain Name Disputes – Cyber squatting
- Explain the functions of Search Engines and their Abuse.
- Discuss the IPR regulatory framework at the National and at International level.

6.2 BASIC CONCEPT: IPRS

The term Intellectual Property can be defined as intangible property which is creations of one's mind and is not merely an idea but an expression of it viz; musical, literary and artistic works; inventions; designs; symbols, names and images. Novelty is considered as the main ingredient for fulfilling the condition of the intellectual property. The rationale behind providing Intellectual Property rights and legal protection to the creators and inventors is to give them, the due recognition for their intellectual work and also the monetary benefits for certain period of time. This will further encourage more innovations; economic and technological growth, facilitate the transfer of technology providing more job opportunities, growth in industry, joint ventures and licensing.

6.2.1 Forms of IPR

There are basically seven forms of intellectual property: copyright and related rights; trademarks, patent, industrial design, geographical indications, trade secrets and plant variety. **(https://www.wipo.int).**

I. **Copyright and related rights**

a. A copyright is used to protect creative literary, musical, dramatic, or other artistic works like cinematographs films and sound recordings inclusive of musical compositions, audio recordings, paintings, photos, sculptures, books, articles, diagrams, movies, website content and even computer software and programmes though the inventions related to software are protected under patent law.

b. **Rights Granted**: provides economic and moral rights. The copyright owner has exclusive rights pertaining to reproduction and distribution of their literary and artistic work; Public performance of the work; Broadcasting of the work; communicating the work to public by wire or wireless means; Commercial rental of the work.

c. **Copyright protection is available** if the work is original and exists in some tangible form based on the national laws. It does not necessarily require registration except for evidence that establishes ownership. The right is granted for specific period and may vary from country to country and from aparticular class of work to another class of work.

II. **Patents**

a) A patent is an exclusive right granted to protect an invention which is a product or a process and can also be applicable to newly engineered plant species or strain however a discovery, scientific theory or mathematical method is excluded from patentability, but its application or use can be patentable.

b) **Rights Granted**: are territorial in nature and patent protection is granted for a limited period.

c) **Patentable and non-patentable inventions** -*An invention is patentable*, if it is Novel, has Inventive step (non- obvious) and capable of industrially application. However, the methods of doing somethinglike book keeping, trading of stocks; Diagnostic, therapeutic and surgical methods for the treatment of humans and animals; Inventions contrary to humanity, public order, morality, public health, environment and safety are not patentable. For example, process of cloning.

d) There are certain products or process which are Novel and have Industrial application and are protected as **Utility Model not as patent**, for a shorter period, generally 10 years and do not require inventive step as the protection requirement like patents.

III. **Trademarks**

a) A trademark is a distinctive sign, word, symbol or mark used in trade to distinguish the goods or services. Trademarks help consumers to identify the source of products or services.It could be name, signature, logo, brand label, phrase, slogan, letter, a numeral or any combination of them.

b) **For registration of trademark,** it should be (i) distinctive in nature (distinguishable from other goods and service). Registration of trade mark is valid for specific period and needs to be renewed.

c) **Registered trademark owner** has exclusive right to use and is also entitled to complete or partial assignments of rights in relation to the mark to another person, including the right to earn royalties.Trade mark owner can also permit restricted use of trademark by way of trademark licensing.

IV. **Industrial designs**

a) Consists of appearance of a product/logo; the shape of an object; composition of design, pattern of cloth. The industrial design may have three-dimensional features, such as the shape or surface of an article, or two-dimensional features, such as patterns, lines or color.

b) **For protection**, an industrial design must be (i) new or original and (ii) aesthetic and requires mandatory registration.

V. **Geographical Indication (GI)**–

a) It is a name or sign used on certain products which corresponds to a specific geographical location or origin (e.g. a region, or country). A Geographical Indication should have special quality or reputation.

b) Geographical indications are typically used for agricultural products, foodstuffs, wine and spirit drinks, handicrafts, and industrial products. Examples: Basmati rice, Swiss watches, Ethiopian coffee, Tequila for spirits produced in Mexico, Electrical appliance Made in UK.

c) In order to function as a GI, a sign must identify a product as originating in a given place and the qualities, characteristics or reputation of the product should essentially be due to the place of origin.

VI. **Trade Secrets**

a) **A trade secret** is any confidential secret information having inherent economic advantage to company and is used in business that gives a competitive edgeby reason of it being secret. Examples include formulae, practice,program, process, recipes, pattern, technique, compilation, method, and device or product mechanism.

b) **To qualify trade secret protection,** no registration is required. However, to protect a trade secret having commercial value the businessesmust limit the number of persons who knows or access the information and get the non-disclosureagreements signed by employees.Trade secret remains valid as long as one does not discover it independently.

Among all the intellectual properties copyright, trademark and patent are three of the most commonly considered intellectual property, but nowadays Geographical indication is also gaining a lot of attention as it is related to specific region or any specific nature of work and by protecting those specific regional work the intellectual rights of those regional people are protected and this protection is promoting the work of all these regional people.

The Information Technology Act, 2000 does not mention any thing about intellectual property rights. On the other hand, it can be taken into consideration that infringement of intellectual property rights is a very common practice in the cyberspace and it is very easy to practice any kind of infringement over cyberspace. There are some categories of intellectual property that needs lawto regulate the protection of intellectual works in cyberspace. They are:

- Intellectual works in digital form can easily be replicated.
- Intellectual works in digital form can easily be transmitted.
- Intellectual works in digital form can easily be modified and manipulated.
- Intellectual works in digital form can easily be form in resemblance or equivalence can easily be created.
- One can easily search anything in digital space and link their own work with someone else's work.

Apart from the infringements stated above, Intellectual property infringements in cyberspace comprise of any unauthorized or unlicensed use of: Trademarks, Trade names, Service marks, Images, Music or sound or literary matter.

☞ **Check your progress 1 Spend 2 min**

1. What is trademark?

.....

.....

.....

.....

6.3 COPYRIGHT ISSUES IN DIGITAL- MEDIUM, MUSIC AND GOODS.

The global usage of Internet makes it feasible for any user to share information in cyberspace through various social media means leading to various concerns and issues related to piracy and counterfeited goods leading to huge monetary losses and as a result fake and pirated products in market**. Gulla, R. K., 2007** has rightly pointed out that "the Internet in a way presents a troublesome situation for copyright holders as the users become mass disseminators of others copyright material and creates disequilibrium between the authors and users".

The copyrights owner has certain rights as discussed above but the reproduction right is considered as very important and a very fundamental right

that grants the copyright owner the right to exclusive right to control the making of a copy of the work or to grant permission for its reproduction. The right to communication to public is also the right of copyright owner however growth in digital technology, use of computer system and networks that allows easy access and transmission of work makes the copyrighted work less distinct and is communicated to the public may lead to infringement of right of the copyright owner.

In cases where the defendant copies cd's onto its servers and do not create any new form of aesthetics, expression but rather to repackage and retransmit the same expression through another medium leads to infringement of copyright as held in *Books, Inc. V. Kinko's Graphics Corp,*1991 that repetition of copyrighted material that "merely repackages or republishes the original" is unlikely to be deemed a fair use. It was retreated in Infinity *Broadcast Corp. V. Kirkwood,* 2d Cir.1998, where court rejecting the fair use defense by operator of a service that retransmitted copyrighted radio broadcasts over telephone lines as cited in the case UMG Recordings, Inc 2000, in this case Utilizing the technology "MP3" which permits rapid and efficient conversion of compact disc recordings ("CDs") to computer files easily accessed over the Internet the defendant or around in January 2000, launched its "My.MP3.com" service, which is advertised as permitting subscribers to store, customize and listen to the recordings contained on their CDs from any place where they have an Internet connection. To make good on this offer, defendant purchased tens of thousands of popular CDs in which plaintiffs held the copyrights, and, without authorization, copied their recordings onto its computer servers so as to be able to replay the recordings for its subscribers. In this case court held that "defendant's "fair use" defense is indefensible and must be denied as a matter of law". Further other affirmative defenses, such as copyright misuse, abandonment, unclean hands-on part of plaintiff, and estoppel, are considered to be essentially frivolous and accordingly disposed of**. (UMG Recordings, Inc. v. MP3.Com, Inc. (harvard.edu**)).

6.4 PATENT MISUSE

A patent ensures total protection of the patented invention under the legal system of a country under the legislation of which it is obtained.

A patent represents monopoly to the patentee that they have the exclusive right to presents to the public the knowledge they have and the patented invention can't be commercially used by any one, or made, distributed or sold without the consent of patent holder. The object of the grant of Patent is to encourage research and development, new innovation and industrial progress. Any kind of practical application in the computer device is known to be patentable but not all software's are patentable but devices like pacemakers are very much patentable, but a computer program is authorized for patenting only

when it contributes to a particular art or a computer program creates a value edition within the existing program and enhances the speed and efficiency of the existing program. In the Indian Patent Law, there is no specific provision pertaining to the protection of software. The United States of America has though recognises the patents for businesses like online stock trading, gambling, e-commerce. Patent can also be misused by patent holder which means an illegal behavior of patentee that leads to violations of the antitrust law or when he tries to expand his product with the actual patent by getting into other licensing agreements. When a patent misuse has been constituted, the patent would be deemed useless. With the advent of digitized media, the various patent infringements are seen in technology industries as given below:

- "Amazon tried to patent its one-click payment option. However, the court decided it was too obvious an idea to patent.
- The file-sharing company Napster settled a lawsuit accusing it of unauthorized distribution of music. It later filed bankruptcy.
- Nintendo was forced to pay a large sum to Tomita Technologies International, Inc. for its 3DS gaming-system technology.
- Microsoft and Google dueled for five years over patent issues involving the Xbox gaming system and Motorola smartphones". (**Famous Patent Infringement Cases (upcounsel.com)**).

6.5 LINKING, IN-LINING AND FRAMING

The Linking, In-lining and framing have become so common since in linking person is providing link and is not making any copies of material available online but the link here allows visitors to bypass information and advertisements at the relevant home page, inlining allows display of graphics on other website and framing often used in conjunction with inlining give picture to picture image and the user can surf directly to the information contained in another site without visiting its home page that may leads to copyright or trademark infringement since it may cause loss of income to businesses; create confusion among the users that the sites endorse each other or are associated with each other which might not be correct and lead to confusion as to original source and loss of reputation and goodwill of the original information holder/ businesses.

""Linking" allows a Web site user to visit another location on the Internet. By simply clicking on a "live" word or image in one Web page, the user can view another Web page elsewhere in the world, or simply elsewhere on the same server as the original page. This technique is what gives the Web its unique communicative power. At the same time, however, linking may undermine the rights or interests of the owner of the page that is linked to. Suppose, for example, that X sets up a homepage for her site. On the homepage she places some advertisements, from which she hopes to make some money. The

homepage also contains links to various subordinate pages, which contain content that X believes consumers wish to see. Y then creates his own Web site, which contains links to X's subordinate pages. The net result is that visitors to Y's site will be able to gain access to X's material, without ever seeing X's advertisements. This type of activity is called "deep linking."" (**Intellectual Property in Cyberspace (harvard.edu)).**

Inlining

""Inlining" is the process of displaying a graphic file on one website that originates at another. For example, inlining occurs if a user at site A can, without leaving site A, view a "cartoon of the day" featured on site B. IMG links -- a special type of link -- can be used to display graphic files on one site that are stored on another". **(Playboy Enterprises v - NYU Law)**

Kelly v. Arriba Soft Corp,2003, a federal court of appeals ruled that it was not an infringement to provide inlined links to "thumbnail" reproductions (here an image search engine called ditto.com used inline links to reproduce full-size photographic images from a photographer's website) based on fair use principlesbut there was no clarity as to whether inlined links to full-sized reproductions constitute an infringement and are not automatically excused as a fair use. In *Perfect 10, Inc. v. Amazon.com, Inc* ,2007, a federal court of appeal again permitted the use of inlined links (reproductions of images from an adult men's magazine website) for thumbnail reproductions.

Framing

""Framing" is the process of allowing a user to view the contents of one website while it is framed by information from another site, similar to the "picture-in-picture" feature offered on some televisions. Framing may trigger a dispute under copyright and trademark law theories, because a framed site arguably alters the appearance of the content and creates the impression that its owner endorses or voluntarily chooses to associate with the framer". **(Playboy Enterprises v - NYU Law).**

In *Futuredontics Inc. v. Applied Anagramic Inc, 2007,* A district court ruled that the addition of the reproduced Web pages within a "frame" by dental website containing contents of other website detailing AppliedAnagramic as well as its trademark and links to all of its Web pagesleads to modificationin the appearance of the linked site and such modifications could, without authorization, amount to infringement of derivative work.

Toavoid linking, framing, and inliningviolations one must seek permission from original owner of content / information /graphics to for deep linking, inlining, pulling full size images and framing graphic links comprising trademarks that tends to side step the linked site's home page and need to sign a linking agreement that give them right to display the Link and trademarks or images in the Link at their Site.In case one could not obtain the required

permission from the linked site, disclaimerclearly and prominently displayed and stating the source of information canreduce the liabilityfor unauthorised use and compensatory damage.

6.6 TRADE MARK ISSUES

Trademark infringement issues arise when some other party uses the trademark having deceptive similarity with the registered trademark of popular brand with intent to confuse consumers as to the producer or manufactures of goods or services. In cases of linking, framing apart from copyright infringement trademark issues also arises. "Attempted enforcement of trademark rights against persons who use marks or content to divert traffic from a trademark owner's site, whether the troublesome use is by friend or foe, requires careful consideration of First Amendment (freedom of speech) concerns as well as of trademark principles of fair use. The public relations nightmare that could result from a misstep in this area should be balanced against both the perceived need to police trademark rights and the proposed policing method." **(Sally M. Abel,1999, p127)**

6.7 DOMAIN NAME DISPUTES – CYBER SQUATTING

Domain name is the internet/web address of a website, is a component of URL (Uniform Resource Locator) which makes it easy to identify the Internet protocol or IP address. It and may represents the trademark of an organization or trade. Trademarks and domain names represent prominent marketing tool, an identity of a business or an organization carrying the goodwill and reputation attached with the business, organization, trade and service. It provides a web address to the trademark in virtual world. For example, in the URL: http://www.ignou.ac.in/ignou/studentzone/results/1, the domain name would be: ignou.ac.in.

Cybersquatting, also known as "domain name hijacking" is a form of domain name misuse and constitutes as an act of registering a domain name with *malafide* intention which is actually someone else' trademark. People create and register domain names of other real owners as their own and take advantage of it by selling them to the real trade owner on excessive price. It is an unscrupulous practicethat leads to misrepresentation in the eyes of potential buyers or services users impacting global trade and infringe the right ofthe particular trademark.

In a famous case, *Yahoo! Inc. v. Akash Arora*, 1999, the defendant created and registered a similar website on domain name "YahooIndia.com" and started providing similar services under the name"Yahoo India" as a trade mark. It

was deceptively identical to the plaintiff's website Yahoo. Inc. which is based in U.S.The High Court of Delhi held that the defendant is liable for deceptively using Yahoo as a domain name and passed an injunction order to restraint the defendant from misusing the trade mark. Thus, trademarks or domain names are equally protected in cyberspace. In*Tata Sons Ltd v. MonuKosuri and others,*2001, the defendant registered the domain name which was deceptively identical to the plaintiff's trademark, "Tata". The court passed an ad interim injunction in favour of the plaintiff. In *Acqua Minerals Ltd. v. Pramod Borse and others*, 2001, the defendant knowingly registered "Bisleri.com" as its domain name who was not the real owner of the trademark. When the real owner came to know about it, they filed an action against the defendant. The court passed an injunction order against the defendant to protect the domain name. **(Seth, 2012,259-260).**

It is considered as the easiest way of IP misuse which is committed in cyberspace and the increasing cases of cybersquatting is becoming a concern for protecting the identity and goodwill over cyberspace. Domain name is beneficial for universal connection as it givesa worldwide recognition. There are many international regulations which gets effected through WIPO to effectively protect a domain name.

☞ **Check your progress 2:** *Spend 2 Min*

1. What is meant by domain name?

.....

.....

.....

.....

6.8 SEARCH ENGINES AND THEIR ABUSE

Cyberspace is a virtual place with endless possibilities, where Internet offers search engine to search and find data in cyberspace. Search engine is a 'searchable index of resources available on internet'. **(Sharma, 2015, 525).**Search engines connects the user with World Wide Web in one place and is a tool which searches online data or content, for example, Google andYahoo. When any website's keyword is searched the user is tuned with the original page of the websites or the domain name. However, there is possibility of unfairness in this process that can lead to trademark infringement issues. The main source of income for such search engine is advertisements showed on the side of the search content. These search engines allow the advertisers to purchase the advertising space on the page of the trademark actually searched

online by the users.These days search engines follow the fashion of showing sponsored ads or links on the webpage searched or the keywords mentioned by the user. Such practice of search engine is objected by trademark owners as violation of trademark in cyberspace being unfair trade practice and misleading. It has potential to create confusion in the mind of the consumer regarding the trademark or keyword searched.

'The *meta tag* helps one to preview that how the webpage will render on the browser. The <meta> tag is placed within the <head> tag, and it can be used more than one times in a document. The metadata does not display on the webpage, but it is used by search engines, browsers and other web services which scan the site or webpage to know about the webpage'**(HTML meta Tag - javatpoint**).

Meta tags do not affect the appearance of a website and are not visible to the Internet user but have been the subject of trademark infringementbecause it can be used by companies in a deceptive manner by putting misleading terms in hidden text or metatags on a web site to divert or confuse e-consumers, internet users where the name of competing companies is substituted with the actual terms that should be used to describing the website. For example, a shoe manufacturing company may bury the meta tag "Bata" in its Web page to lure internet users searching for Bata products.Besides the infringement issues, the exercise of territorial jurisdiction over a domain name dispute and choice of law is the major concern.

It is clear that the ranking over cyberspace can be manipulated and distorted with the help of some illegitimate tricks. Therefore, a proper legal recourse is necessary to overcome all such issues related to the search engine manipulation and the consumers have to remain aware and be conscious at all times about the fact that the information they are getting by using any search engine can be misleading.

☞ **Check your progress 3:** *Spend 2 min*

1. Enlist copyright issues in cyberspace.

.....

.....

.....

.....

6.9 REGULATORY FRAME WORK- NATIONAL AND INTERNATIONAL SCENARIO

6.9.1 Legal Protection in India

IPR Issues in Cyber Space

The internet has created a new virtual world and Information Technology Act, 2000 maintains that world in cyberspace by giving protection to various legal challenges and their suitable solution. Intellectual Properties such as copyright, trademark, patent, layout and circuit designs are the new members of this virtual world which exists in the cyberspace. Therefore, the protection of these rights is as essential as any other right within the cyberspace and with the ever-changingtimes, the demand for protection and remedies is also changing and the need of new and effective law to protect the new inventions is in demand**.(Aiswarya etall ,2018).**

Copyright -In India copyright law is governed by Copyright Act 1957 as amended from time to time. The act prohibits the unauthorized acts of making Xerox copy of a book, copying a computer software program, and incorporation of a portion of another's song into a new song. TheCopyright Act is applicable to original Literary, Dramatic, Musical, Cinematograph films, sound records and Artistic works (*see sec 13 of copyright act*). It also covers Anonymous and pseudonymous works and Posthumous work at presents the act is compatible with Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement and is in harmony with WCT and WPPT. *Section 52 of the Copyright Act, 1957* includes in itself the principle of limitation and exception to infringement of copyright as envisaged under Article 10 of WCT. The acts allow fair use /fair dealing of a literary, dramatic, musical or artistic work (not including a computer program) for the limited use like for private and personal use including research, criticism or review whether of that work or of any other work, reporting current events, for the purpose of a judicial proceeding / a report of a judicial proceeding.The section further provides that the following acts do not amount to copyrights infringement;-(a)making of copies or adaptation of a computer Programme by the lawful possessor of a copy of such computer Programme from such copy in order to utilize the computer Programme for the purpose for which it was supplied or to make back-up copies purely as a temporary protection against loss, destruction, or damage in order only to utilize the computer Programme for the purpose for which it was supplied;(b) the doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer Programme with other programmed by a lawful possessor of a computer Programme, if such information is not otherwise readily available;(c) in the observation, study or test of functioning of the computer Programme in order to determine the ideas and principles, which underline any elements of the Programme while performing such acts necessary for the functions for which the computer Programme was supplied; (d) making of copies or adaptation of the computer Programme from a personally legally obtained copy for non-commercial personal use.Thus,the Copyright, can be assigned or transferred or the owner of the work can license specific uses to another person and accordingly specify the gravity of ownership being given to another

person.The Copyright expires after 60 years from the end of the calendar year in which the author diesLiterary, dramatic, musical or artistic works; The Copyright shall subsist until 60 years from the beginning of the calendar year following the year in which the film/sound recording /photographs/computer programs is made available or first published as the case may be to the public.

The act provides economic rights under sec 14 of act to commercially exploit his creationand also grants moral rights as envisaged under Section 57 of the Act which are special rights of the author of the work viz., (i) Right to claim authorship of the work; and (ii) Right to restrain or claim damages in respect of any distortion, mutilation, modification or other act in relation to the said work if such distortion, mutilation, modification or other act would be prejudicial to his honor or reputation ("Right Against Distortion"). The moral rights can also be exercised by legal representatives post death of the author. As per the Amendment, the right against distortion is available even after the expiry of the term of copyright.

With the advent of the information technologies and Internet, copyright disputes infringement of copyrighted works in digital medium do arise but the existing Copyright Law is also applicable to copyright challenges arising due to use of digitaltechnologies and Internetand can be construed to cover electronic publication. In addition to the Copyright Act, 1957, there is also Copyright Rules, 1958 and the International Copyright Order, 1999. The Copyright Rules contain the rules and regulations and provides various procedures and where, the International Copyright Order is concerned, it deals with the protection of copyright works of nationals of various foreign countries.

Patent- It is governed by the Patents Act 1970; Patents Rules 1972. Section 2(m) of the Patent Act, 1970 provides for the definition of Patent which states that: - "*Patent means patent for any invention granted under this Act".*
To strengthen the patent law, India became signatory to many international agreements like Trade Related Intellectual Property Rights (TRIPS), Paris Convention and the Patent Cooperation Treaty and Budapest Treaty. The Act provides for period of 20 years for every patent from the from the date of application of patent irrespective of whether it is filed with provisional or complete specification. However, in case of applications filed under PCT the term of 20 years begins from the International filing date accorded under PCT.Under the Patent Act, both processes and products are entitled to qualify as inventions if they are new, involve an inventive step and are capable of industrial application. however before grant of patent, Act allows both pre-grant and postgrant opposition. Section 48 of the Indian Patents Act 1970, confers exclusive rights upon the patentee to exclude third parties from making, importing, using, offering for sale or selling the patented invention, patented product or patented process and use of patented invention without the

prior permission from the patent holder may amount to infringement. the patent owner can however grant permission in the form of a license.

It is interesting to note that in some countries Industrial design is also protected under patent, because these designs are created with some specific purpose and they impact consumers' choice between products. According to World Intellectual Property Organization (WIPO), industrial designs impact marketability and commercial value of product

☞ **Check your progress 4:** *Spend 2 Min*

1. What is termed as 'patent' according to the Patent Act, 1970?

.....

.....

.....

.....

Trademark-Trade Marks Act (TMA), 1999 protects the rights of the trademark owners or business entities for a term of 10 **years** from the date of application, renewable every 10 years on payment of the requisite fee.Sec 135 of the provides remedy in suits for infringement or for passing off in form of injunctions and damages. Section 103 imposes penalty for applying false trademarks, trade descriptions which shall be punishable with imprisonment for a term not less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees. Further, section 104 of TMA imposes penalty for selling goods or providing services to which false trade mark or false trade description is applied punishable with imprisonment for a term not less than six months which may be extended to three years and with fine which shall not be less than fifty thousand rupees which may be extended to two lakh rupees. In cases where trademark is unregistered in such situation common law remedy of passing off is provided to the owner of the trademark. Section 29 of the Trademark Act, 1999 deals with circumstances leading to infringement of registered trade mark as where person affixes it to goods or the packaging thereof; offers or exposes goods for sale, puts them on the market, or stocks them for those purposes under the registered trade mark, or offers or supplies services under the registered trade mark; imports or exports goods under the mark; or uses the registered trade mark on business papers or in advertising. Section 29(7) deals with violation of trade mark through labelling or packaging goods, as a business paper, or for advertising goods or services, advertising , Sec27(8) provides that a registered trade mark is infringed by any advertising of that trade mark if such advertising(a) takes unfair advantage of and is contrary to honest practices in industrial or commercial matters; or(b) is

detrimental to its distinctive character; or (c) is against the reputation of the trade mark. **(www.indiankanoon.org).**

Three types of remedies are available against infringement of IPR 1. *Civil Remedies*- injunctions, damages, rendition of accounts, exparte order, seizure, destruction or forfeiture of infringing goods. 2. *Criminal remedies*- section 63 of the Copyright Act, 1957 deals with Offences of infringement of copyright and Chapter XII of the Trademarks Act, 1999 deals with offences, penalties and procedures pertaining to trademark infringement. 3. *Administrative Remedies*- import/ export of goods including protection of patents, trademarks and copyrights under Indian Customs Act, 1962; Confiscation of infringing material by Custom Authorities; Restrictions against parallel importation of goods.

Trademark infringement through search engine is also subject of trademark litigation. Considered as unfair trade practice and a matter of great concern for judiciary to provide adequate protection to trademark owners in digitized medium. The advancement of digital technology, therefore presents legislators with a choice, either to expand or modify the existing law taking into account the new concerns that emerged due to cyberspace.

The following laws govern other form of IPR for ex: Designs Act, 2000 deals with laws relating to Industrial Designs; The geographical Indications of (Registration and Protection) Act, 1999 for Laws relating to Geographical Indication; Information Technology Act, 2000 deals with electronic records.

☞ **Check your progress 5:** *Spend 2 min*

1. What remedies are available against infringement of IPR?

.....

.....

.....

.....

6.9.2 International scenario

Important treaties which provide international protection to Copyright are: -

i. Berne Convention for protection of Literary and Artistic Works, 1886.
ii. Universal Copyright Convention, 1952
iii. Agreement on Trade Related Aspects of Intellectual Property Rights, 1994.

The purpose of making these treaties is to create uniformity in dealing with the disputes related to the Intellectual Property Rights, because copyright is governed within the country according to the internal laws of the country and with the help of these treaties, uniform protection is given to all member

countries of that particular treaty. It is an important remedy against infringements and provides protection to copyright internationally. India is a member country to these treaties and has given protection against all member countries if any infringement of the copyright takes place. However, the registration process of the copyright may differ from one member country to another member country.

The Universal Copyright Convention (UCC) -was adopted in 1952 under the support and protection of United Nations Educational, Scientific and Cultural Organization (UNESCO) with a view to extend international copyright protection universally. After the entry into force of the Revision Act, in 1971, the members have to strictly comply in accordance to the revised version. The Intergovernmental Copyright Committee has been also established in compliance with Art. 11 of the UCC consisting of the representatives of 18 Contracting States. (**Universal Copyright Convention. United Nations Educational, Scientific and Cultural Organization (unesco.org))**

Berne Convention-

The Berne Convention deals with the protection of works and the rights of their authors. It is based on three basic principles: (1)Works originating in one of the Contracting States (that is, works the author of which is a national of such a State or works first published in such a State) must be given the same protection in each of the other Contracting States as the latter grants to the works of its own nationals (**principle of "National treatment"),** (2) Protection must not be conditional upon compliance with any formality (principle of "**Automatic" protection),(**3) Protection is independent of the existence of protection in the country of origin of the work (**principle of "Independence" of protection**). If, however, a Contracting State provides for a longer term of protection than the minimum prescribed by the Convention and the work ceases to be protected in the country of origin, protection may be denied once protection in the country-of-originceases. Berne convention contains a series of provisions determining the minimum protection to be granted, as well as special provisions available to developing countries that want to make use of them. The Berne Convention allows certain limitations and exceptions on economic rights, that is, cases in which protected works may be used without the authorization of the owner of the copyright, and without payment of compensation. These limitations are commonly referred to as "free uses" of protected works, and are set forth in Articles 9(2) (reproduction in certain special cases), 10 (quotations and use of works by way of illustration for teaching purposes), 10bis (reproduction of newspaper or similar articles and use of works for the purpose of reporting current events) and 11bis(3) (ephemeral recordings for broadcasting purposes).As to the duration of protection, the general rule is that protection must be granted until the expiration of the 50th year after the author's death. There are, however, exceptions to this general rule. In the case of anonymous or pseudonymous

works, the term of protection expires 50 years after the work has been lawfully made available to the public, except if the pseudonym leaves no doubt as to the author's identity or if the author discloses his or her identity during that period; in the latter case, the general rule applies. In the case of audiovisual (cinematographic) works, the minimum term of protection is 50 years after the making available of the work to the public ("release") or – failing such an event – from the creation of the work. In the case of works of applied art and photographic works, the minimum term is 25 years from the creation of the work. **(https://www.wipo.int/treaties/en/ip/berne/summary_berne.html).**

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), it provides that the principles of national treatment, automatic protection and independence of protection also bind those World Trade Organization (WTO) Members not party to the Berne Convention. In addition, the TRIPS Agreement imposes an obligation of "most-favored-nation treatment", under which advantages accorded by a WTO Member to the nationals of any other country must also be accorded to the nationals of all WTO Members. Under the TRIPS Agreement, an exclusive right of rental must be recognized in respect of computer programs and, under certain conditions, audiovisual works. Under the TRIPS Agreement, any term of protection that is calculated on a basis other than the life of a natural person must be at least 50 years from the first authorized publication of the work, or – failing such an event – 50 years from the making of the work. However, this rule does not apply to photographic works, or to works of applied art. (**https://www.wipo.int/treaties/en/ip/berne/summary_berne.html).**

The U.S. Copyright Act states that a copyright exists once an "original work of authorship [is] fixed in any tangible medium of expression . . . from which [it] can be perceived, reproduced or otherwise communicated."**17 U.S.C. 102(a).**Copyright owners (or their assignees) have the right to carry out or authorize reproduction and distribution of their work; preparation of derivative works; and, for literary, musical, and various visually based works, the public performance or display of their work. Copyright law also imposes limitations on the exclusive rights that copyright owners enjoy during the life of a copyright. Some of those limitations apply to the use of a particular product, such as consumers' ability to make an archival copy of a computer program without authorization of the copyright owner**(17 U.S.C. 117).**

The Digital Millennium Copyright Act (DMCA), 1998

'The Act modifies the details of copyright law in a variety of ways, including instituting a royalty-setting process for Internet music broadcasts (Webcasts) and specifying exemptions for library and archival copying. It also established two major provisions of current digital copyright law—the ant circumvention prohibitions and the safe-harbor requirements for Internet Service Providers (ISPs)—that are intended to enhance the ability of copyright owners to protect

their work from infringing uses and to identify and prosecute those users found to be infringing copyright. The DMCA makes it illegal to circumvent a technology that controls access to copyrighted materials—for example, an encryption program that prevents unauthorized viewing of a movie on the Internet."[17 U.S.C. 1201(a)(1).]. The DMCA further prohibits manufacturing or trafficking in products "primarily designed or produced for the purpose of circumventing" technologies that are designed either to control access to copyrighted material (as in the previous example of a movie distributed via the Internet) or to prevent the use of such material in an infringing way. [17 U.S.C. 1201(a)(2) and (b)].In contrast, the DMCA does permit some circumvention activities or products that do not infringe copyright. For example, copyright law explicitly recognizes copying a computer program for archival purposes as a limitation on the exclusive rights of owners of copyright on computer programs. Hence, if a manufacturer of computer programs applied a copy-control technology to prevent unauthorized copying of its product, a lawful purchaser could legally circumvent that technology to make an archival copy. The example of software copying illustrates a central principle of copyright law: copyright owners have no legal obligation to facilitate any activity that qualifies either as a limitation on their exclusive rights or as fair use generally. At the same time, if the DMCA's prohibitions are to be effective legal instruments for deterring infringement, copyright owners must take measures to protect their intellectual property from unauthorized access and use. Thus, the fair use and other consumer concerns, such as personal privacy on the Internet was taken into account while crafting the anticircumvention provisions. However, technological progress is placing growing strains on whatever balance had previously been achieved between the rights of copyright owners and the interests of consumers.' **(Copyright Issues in Digital Media, Aug2004).**

International Patent protection Regime- There are many Patent-related treaties: WIPO-administered treaties; Paris Convention (concluded 1883); Patent Cooperation Treaty (1970); Strasbourg Agreement (1971); Budapest Treaty (1977): Patent Law Treaty (2000);WTO TRIPS Agreement (1994); Treaties outside WIPO; Regional treaties. Many inventors and other patent owners provide products or services around the world. However, the protection of a patent granted by the U.S. Patent and Trademark Office ends at the U.S. border and cannot be usedin other countries to prevent the use of the particular invention, owner of the patent needs to seek individual protection in each of the country in absence of any single international patent. But if both the foreign national's home country and the country granting the patent have signed an international treaty the rules of reciprocity to file patent application may apply that requires a country that issues a patent to a foreign national to provide the foreign national with the same rights as a patent owner that a citizen of that country will have. For example, most of the nations have signed the *Paris Convention*that deals with reciprocal rights in relation to patent

applications though an inventor still needs to file a separate application in each country that has signed the Convention, but each country will use the U.S. filing date for the application and to get advantage of this protection, a U.S. inventor must file their application in the foreign country within a year of filing in the U.S and the inventors of design patents must file application within six months of the U.S. filing.However, filing for multiple patents to enforce one's patent rights in foreign countries by way of infringementsuits is very expensive including hiring of lawyer fee.(**International Patent Law and Protection. Justia)**

The Patent Cooperation Treaty is another international treaty that allows patent protection for an invention simultaneously in each of a large number of countries by filing an "international" patent application. Such an application may be filed by anyone who is a national or resident of a PCT Contracting State.t may generally be filed with the national patent office of the Contracting State of which the applicant is a national or resident or, at the applicant's option, with the International Bureau of WIPO in Geneva. If the applicant is a national or resident of a Contracting State party to the European Patent Convention, the Harare Protocol on Patents and Industrial Designs (Harare Protocol), the Bangui Agreement, or the Eurasian Patent Convention, the international application may also be filed with the European Patent Office (EPO), the African Regional Intellectual Property Organization (ARIPO), the African Intellectual Property Organization (OAPI) or the Eurasian Patent Office (EAPO), respectively. The Treaty regulates in detail the formal requirements with which international applications must comply. Filing a PCT application has the effect of automatically designating all Contracting States bound by the PCT on the international filing date.The international application is subjected to an international search. (**Summary of the Patent Cooperation Treaty (PCT) (1970) (wipo.int))**

Protection in cases of Domain Name Disputes-The WIPO provides for the effective and speedy online complaint resolution mechanism and relief to the victim in cases of domain name disputes which is known the 'Uniform Domain Name Dispute Resolution Policy' adopted by ICANN on October 24, 1999.

The procedure introduced by the policy allows trademark owners to settle cases of disputed domain name registration without resorting to national courts. On ICANN's authorization, the WIPO Arbitration and Mediation Centre started offering its services for resolving the issues. **(Sople, 2016, 287).**
"All registrars must follow the Uniform Domain-Name Dispute-Resolution Policy (often referred to as the "UDRP"). Under the policy, most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name. Disputes alleged to arise from abusive registrations of domain names (for example, cybersquatting) may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by

filing a complaint with an approved dispute-resolution service provider.To invoke the policy, a trademark owner should either (a) file a complaint in a court of proper jurisdiction against the domain-name holder (or where appropriate an in-rem action concerning the domain name) or (b) in cases of abusive registration submit a complaint to an approved dispute-resolution service provider".**(Uniform Domain-Name Dispute-Resolution Policy - ICANN).**

6.10 SUMMARY

The terms Intellectual Properties and Cyberspace is entirely different but in digital world almost every information is available over cyberspace and because of this many of the intellectual property works are getting infringed or being misused which results in consumers being misled and violation of the rights of the owners of the intellectual property. The rationale behind providing Intellectual Property rights and legal protection to the creators and inventors is to give them the due recognition for their intellectual work and also the monetary benefits for certain period of time to encourage further innovations; economic and technological growth but the IPR violations in digital media like Copyright's violations, Deep Hyper linking, Framing, abuse of search engines by use of Meta-tags, spamming and especially trademark violation giving rise to Domain Name Disputes are major concerns. Therefore, Management of Intellectual Property rights in cyberspace is an important issue to combat property infringements in the virtual space. It is seen that conventional laws for protecting intellectual property in India and at International level is also applicable to the infringements taking place in cyberspace.

6.11 SOLUTION/ANSWERS

Check your progress

1. A trademark is a distinctive sign, word, symbol or mark used in trade to distinguish the goods or services. Trademarks help consumers to identify the source of products or services. It could be name, signature, logo, brand label, phrase, slogan, letter, a numeral or any combination of them.
2. The domain name is a component of a uniform resource locator (URL) used to access web sites, for example: URL: http://www.example.net/index.html. It is Top-level domain,i.e . net. Domain name: example.net.
3. The following IPR issues arises in cyberspace: Copyright issues; Patent's infringement; Linking, In-lining and framing; Trade Mark

disputes including domain Name Disputes – Cybersquatting and abuse of Search Engines.

4. As per section 2(1)(m) of Patent Act, 1970 patent means a patent for any invention granted under this Act.
5. Civil Remedies- injunctions, damages, rendition of accounts, exparte order, seizure, destruction or forfeiture of infringing goods. 2. Criminal remedies- section 63 of the Copyright Act, 1957 deals with Offences of infringement of copyright and Chapter XII of the Trademarks Act, 1999 deals with offences, penalties and procedures pertaining to trademark infringement. 3. Administrative Remedies- import/ export of goods including protection of patents, trademarks and copyrights under Indian Customs Act, 1962; Confiscation of infringing material by Custom Authorities; Restrictions against parallel importation of goods.

6.12 REFFERENCES/FURTHER READINGS

- Acqua Minerals Ltd. v. Pramod Borse and others (2001 PTC 619).
- Ahuja V. K (2017).*Law related to Intellectual property rights*. 3rd ed. LexisNexis.
- Aiswarya etall (2018). IPR and Cyberspace-Indian Perspective with Special Reference to Software Piracy. *International Journal of IPR regulatory framework*.119 (17), 1677-1692.
- Books, Inc. v. Kinko's Graphics Corp., 758 F.Supp. 1522, 1530-31 (S.D.N.Y.1991)
- Consim Info Pvt Ltd v. Google India Pvt. Ltd. Retrieved on March 10, 2020 from https://indiankanoon.org/doc/155459494/.
- Controller General of Patents, Designs & Trademarks (2020). Retrieved from http://www.ipindia.nic.in/patents.htm
- Copyright Issues in Digital Media (Aug2004). The Congress of the United States Congressional Budget Office. Retrieved from https://www.cbo.gov/sites/default/files/108th-congress-2003-2004/reports/08-09-copyright.pdf
- Futuredontics Inc. v. Applied Anagramic Inc (1997 46 USPQ 2d 2005) ;(C.D. Calif. 1997).
- Gogoi, C. Trademark Infringement through Keyword Advertising in India: Issues and Challenges. Retrieved March 10, 2020, from http://docs.manupatra.in/newsline/articles/Upload/.
- Gulla, R. K. (2007). Digital Transformation of Copyright Laws and the Misty Indian Perspective. *Icfai Journal of Intellectual Property Rights*. 6(3), 1-26.
- HTML metaTag - javatpoint. Retrieved from https://www.javatpoint.com/html-meta-tag

- International Patent Law and Protection. Retrieved from https://www.justia.com/intellectual-property/patents/international-patent-protection/.
- Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).
- Linking, Framing, Meta Tags, and Caching. Retrieved from https://cyber.harvard.edu/property00/metatags/main.html
- Nolo eCommerce Center. Linking, Framing and Inlining. https://www.garage.com/resources/reference-library/internet-law/linking-framing-and-inlining/
- Perfect 10, Inc. v. Amazon.com, Inc. CV-05-04753-AHM (9th Cir., May 16, 2007).
- Playboy Enterprisesv - NYU Law. Retrieved https://www.law.nyu.edu/sites/default/
- Rich stim. Connecting to Other Websites - Copyright Overview. Stanford Copyright and Fair Use Center. *Stanford Libraries Home*, Justia, NOLO, LibraryLaw.com &Onecle.
- Saha.S (2012).*Challenges to Intellectual Property Rights in Cyberspace*.LAP Lambert Academic Publishing .
- Sally M. Abel (1999). Trademark Issues in Cyberspace: The Brave New Frontier. 5 *MICH. TELECOMM. TECH. L. REV*:91. Retrieved from https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1158&context=mttlr; https://assets.fenwick.com/legacy/FenwickDocuments/Trademark_in_Cyberspace.pdf
- Seth, k. (2012). *Computers, Internet & New Technology* (1st ed.). Nagpur: Lexis Nexis Butterworths Wadhwa.
- Sharma, V. (2015). Information Technology Law & Practice: Law & Emerging Technology. *Cyber Law & E-Commerce* (4th. ed.). New Delhi: Universal Law Publication.
- Sople, V. (2016). *Managing Intellectual Property: The Strategic Imperative* (5th ed.). Delhi: PHI Learning Pvt. Ltd.
- Summary of the Patent Cooperation Treaty (PCT) (1970). Retrieved from https://www.wipo.int/treaties/en/registration/pct/summary_pct.html.
- Tata Sons Ltd v. MonuKosuri and others (2001 PTC432.).
- UMG Recordings, Inc v. MP3.com, Inc., No. 00 Civ. 472(JSR). United States District Court, S.D. New York., May 4, 2000. Retrieved from https://h2o.law.harvard.edu/cases/2623.
- Uniform Domain-Name Dispute-Resolution Policy - ICANN. Retrieved from https://www.icann.org/resources/pages/help/dndr/udrp-en.

- Universal Copyright Convention. United Nations Educational, Scientific and Cultural Organization. Retrieved from http://www.unesco.org/new/en/culture/themes/creativity/creative-industries/copyright/universal-copyright-convention/.
- WIPO. Retrieved from https://www.wipo.int/edocs/mdocs/africa/en/wipo_tiscs_kla_17/wipo_tiscs_kla_17_t_4.pdf
- Yahoo! Inc. v. Akash Arora, (78(1999) DLT 285).