Chapter I

Introduction
CHAPTER – I
INTRODUCTION

The eminent English jurist Salmond has rightly observed that law seeks to regulate the conduct of individuals in the society.\(^1\) It is therefore, the result of progress and development of the society. The evolution of law can be historically traced back from the origin of civil society. With the gradual development of society, people started living and working together, forming groups which eventually led to the formation of the State. There was need for regulating the conduct of individuals inter se; therefore, State formed the rules of governance which later came to known as ‘law’.

Thus development of law is a process which continued with the changes and advancement in the societal circumstances. Law is generally made to meet the needs of the society and therefore, it is a dynamic concept which undergoes changes with the changing needs of the society. The modern technological evolution has enabled human society to prosper and progress but at the same time has given rise to new problems which were hitherto not known to mankind and cyber criminally is one such grey area which emerged only a few decades ago. The tremendous progress made by computer technology during the last quarter of the 20\(^{th}\) century has now made it possible for the people to visually chat, send messages, transmit information and conduct business with a person in any part of the world through internet. The computer as an innovative mechanism has increased our capacity to store, search, retrieve and communicate data as also accessibility to information which has made it possible for us to communicate with any person, anywhere, anytime in the world.

\(^1\) Fitzgerald P.J. Salmond on Jurisprudence (12th ed) p.3
Need for a Cyber Law

The information technology advanced by computer network undoubtedly pervades every aspect of society and governance in the present new millennium. With the increased dependence of e-commerce and e-governance, a wide variety of legal issues related to use of internet as well as other forms of computer or digital processing devices such as violation of intellectual property, piracy, freedom of expression, jurisdiction etc. have emerged, which need to be tackled through the instrumentality of law.

The word cyberspace is believed to have been coined by author William Gibson in his sci-fi novel ‘Neuromancer’. Gibbson visualized the cyber space in these words:

“A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts……. A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, lines of light ranged in the non-space of the mind, clusters and constellations of data”.  

Since cyberspace has no geographical limitations or boundaries nor does it have any physical characteristics such as, sex, age, etc., it poses a big challenge before the law enforcement agencies or regulating cyberspace transactions of citizen within a country’s territorial jurisdiction. Though in practical terms, an internet user is subject to the laws of the State within which he/she goes online but this general rule runs into conflict where the disputes are international in nature.

---

3 The word ‘cyberspace’ was used for the first time by Willaim Gibson in his science fiction ‘Neuromancer’ in 1982. It may be conceptually described as communication over the internet connected by some kind of technology.
It is true that at the time when computer technology was at its developing stage, no one ever contemplated that it can be indiscreetly misused by the internet users for criminal purposes. Because of the anonymity of its character and least possibility of being detected, the cyber criminals are misusing the computer for a variety of crimes which calls for the need for an effective legal framework and regulatory measures to prevent the incidence of this peculiar type of criminality which is rampant in cyberspace.

**Development of Cyber Crime**

Commenting on the information technology revolution which has transformed the world into a global community, Walter B Wriston observed, “technology has made us a ‘global community’ in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long”.  

The advancement of technology has brought about radical changes in the modern society. But human experience has shown that every technological change brings with it some unforeseen problem, taking advantage of which the law breakers explore new techniques to perpetrate their criminal activities. In fact, technology-generated crimes not only affect individuals or a nation, but have a widespread ramification throughout the world. Internet is one such gray area, which has given rise to the menace of cybercrimes. The computer based global communication

---

system has crossed the territorial borders thus creating a distinct field for online criminal activity warranting global attention.

Cybercrimes have emanated from development of computer network. Internet in the present millennium has become all pervasive and omnipresent. It has also brought with it new problems hitherto unknown to humanity. Internet in sense is analogous to the “high seas” which no one owns yet people of all the nationalities use it. The term ‘cybercrime’ encompasses within it a variety of criminal activities taking place in the cyberspace through the media of global communication and information via internet.

It is an inevitable evil having its origin in the growing dependence of mankind on computers in modern life, the reason being that the computers despite being high technology devices are extremely vulnerable. Thus, whenever any crime or criminal activity takes place with the use of computer, it constitutes a cybercrime. It is for this reason that ‘cybercrime’ has been defined as “an unlawful act wherein the computer is either a tool or a target or both”\(^5\).

Cybercrimes are such harmful activities in the cyberspace which may cause damage to a person, property or even the State or society as a whole. There are many cybercrimes which are being committed by offenders all over the world using computer technology.

Being radically different from the conventional crimes, the law enforcement agencies find it difficult to tackle cybercrimes with the existing infrastructural mechanism because of lack of adequate knowledge about the computer operating systems. This is the main reason why this relatively new variety of crime is posting a challenge to the legal

\(^5\) Supra Chapter 1.
regime. The problem has been further aggravated by the introduction of internet.

The menace of cyber criminality is not confined to one or two countries but the whole world is facing this gigantic problem as a “technological scorn”. India is no exception to this computer generated menace. However, as a measure to prevent and control internet crimes, the Parliament enacted the Information Technology Act, 2000 which came into force on October 17, 2000. The Act categorically defines relating to cyberspace such as tempering with computer source document, hacking with computer system, breach of confidentiality and privacy etc.

It is not that prior to this legislation there was no law to deal with these offences. The Indian Penal Code, 1860 already contained provisions to prevent and control cybercrimes but they were not found to be sufficient enough to tackle all varieties of cyberspace crimes. The obvious reason being that no one knew about the computer or internet at the time when the Indian Penal Code was enacted.

It hardly needs to be stated that science and technology has extended its tentacles cutting across the national frontiers whereas the law is still struggling to define and redefine the boundaries for the control of cybercrimes. Following a similar course, the cyber law particularly, the Information Technology Act is engaged in prevention and control of cybercrimes within the country’s territorial jurisdiction overlooking the fact that cyber criminality is a global phenomenon which has no territorial limits.

---

6. The Computer Technology has mainly developed and expanded throughout the world only during the last quarter of 20th Century.
Global View of Cyber Crime

Cybercrimes being global in character, generally affects the person far away from the place of offence, may it be in the same country or some other country. It therefore, requires policing at international level as also the active co-operation of the international community. The European Convention on Cybercrime\(^7\) was indeed a praiseworthy attempt as it laid down guidelines to be followed by the member States in combating cybercrime. The Convention suggested measures to be initiated by the States for restructuring their cyber laws to meet the new challenges.

The Convention not only dealt with the changes and improvements in the substantive part of criminal law but also referred to the procedural aspect which must be taken into consideration while restructuring the existing law to meet the current needs of developing technology. It has been generally accepted that procedural aspect of criminal law is the main hurdle in tackling the problem of cybercrime effectively but at the same time, the substantive part of cybercrime also needs to be redefined to fight against ongoing cyber criminality.

Out of a variety of cybercrimes, the European Convention has chosen ten specific cybercrimes\(^8\) and urged the member States to include them in their information technology laws and provide a concrete mechanism to fight against them. But it is rather unfortunate that many cybercrimes of a particular country are not treated as crime under the criminal law of other countries, which really poses a problem when cross-country cybercrimes are involved. The solution to this problem lies in enacting a global cyber law uniformly applicable to all the countries of the world. The crux of the matter is that universally accepted standard

---

7. Effective from June, 2001
8. Section 1, Chapter II of the European Convention document which contains Articles 2 to 13 defining ten cybercrimes under five separate titles.
cybercrime preventive laws should not vary from place to place. In other words, uniformity be ensured with reference to substantive cyber laws of various nations.

An overall global view of cyber law indicates that many countries do have their national legislation for combating cyber criminality, but they radically differ from each other as a result of which, a particular cyberspace activity which is considered as a criminal offence in one country may not be necessarily so in another country. This variation in law provides loopholes for the cyber offenders to escape punishment.

Therefore, there is dire need for international cybercrime legislation which could be uniformly acceptable by all the countries to tackle the problem of cybercrime. Not only that, there should also be an international policing agency for countering cyber offences. The solution to the problem therefore, lies in the concerted and united efforts of nations around the world and their mutual co-operation in fighting against cyber criminality.

Broadly speaking, the law enforcement agencies all over the world are confronted with four major problems while dealing with cybercrimes in a network environment. The detention and prosecution of cyber criminals online is hindered by the challenges, which may be technical, legal, operation and jurisdictional.

As regards technical challenges, cybercrimes such as hacking of a website, stealing data stored in computers, espionage, exchange of pornographic material, blackmailing etc. involve detection of source of communication which is a complicated task. Therefore, the cyber criminals find it easy to impersonate on the internet and hide their identity.
Legal Challenge and Cyber Criminality

The legal challenge emerges from the fact that cyber criminality is not longer confined to the developed countries alone but it has assumed global dimensions in recent decades. The conventional legal techniques of investigation of cybercrimes are inadequate particularly, in case of cross-country crimes. The problem becomes more complex because of lack of any universally accepted definition of cybercrime.

Therefore, a cybercrime in a country may not necessary be a crime in another country. There are hardly twenty countries in the world which have enacted comprehensive cyber laws. In the absence of an adequate cybercrime laws, the cyber criminals carry on their illegal activities undeterred. Therefore, effective handling of cybercrimes requires a legal framework which is equally applicable to all the countries. The cyber laws should also be responsive to the fast developing information technology. The internet has enabled the cyber offenders to target maximum number of people at a minimal cost merely at the click of a button. Therefore, cyber security assumes utmost importance.

Operational Challenges and Cyber Criminality

The operational challenges faced by the law enforcement agencies because of lack of adequate cyber forensic technology for dealing with cybercrimes constitute another in-road which renders it difficult to collect and preserve sufficient evidence against the person accused of cybercrime, thereby resulting in his/her acquittal by the court. The traditional modes of procuring evidence are unsuited in case of cybercrime investigation because most of evidence exists in electronic form. Therefore, there is dire need to develop suitable computer forensic mechanism for effective handling by cybercrime investigation.
In the context of electronic evidence, it is significant that despite the fact that digital signatures have facilitated e-commerce by reducing paper-work and ensuring quick transactions, it has not been widely accepted in India because of the technicalities involved in it and therefore, people in general still believe that paper-based documents are more dependable and trustworthy than the paperless electronic records.

The reason being that former are tangible and serve as best piece of evidence before a law court. However, with the expansion of e-commerce and legal recognition of e-contracts in business transactions, there is change in the mindset of the people and they are gradually adapting themselves to the new e-environment and finally switching over to paperless electronic transactions.

**Jurisdictional Challenges and Cyber Criminality**

The Jurisdictional challenges impeding the efficient handling of cybercrime investigation result out of widespread inter-connectivity of the computer networks and the supporting infrastructure such as telecommunication, information dissemination on website etc. In fact, jurisdiction is a broad concept which refers to whether a court has the power to adjudicate, i.e. whether it has personal jurisdiction to try the case and territorial jurisdiction over the location or place where the crime is committed or the parties concerned reside. In case of cross-country cyber dispute or crime, the problem often arises as to the law of which country would be applicable to the case in hand.

**Objective of the Study**

In the era of globalisation and information technology cyber space has reduced distances. Law has to keep pace with the development of information technology. Cyber and internet system has brought many a
problems too. Cyber crimes have virtually crossed the geographical boundaries. Looking to the reported increasing trends of cyber crimes in India and world around, it has become a matter of serious concern that if effective statutory and other regulatory measures are not adopted in due course than there are reasonable apprehensions the tentacles of cyber crimes would engulf the entire society.

The researcher has endeavoured to undertake the present working in search for such solution which could help in controlling and curbing cyber crime.

In this work the researcher proposes to draw her own views and conclusions which may be helpful for controlling and curbing cyber crime under laws and making the present law efficient enough to meet the future challenges of the society and ultimately our country.

**Research Methodology**

Research Methodology for proposed research work shall be doctrinal analytical study. Critical analysis of statutory enactments that is IT Act, 2000 as well as analysis of various statutes operating in the field shall be made. The Judicial pronouncements of various courts in India as well as under prominent jurisdictions of the world would also be thoroughly examined by the researcher in the instant study.

The present study shall collect, collate and analyze different Judicial decisions of various courts. Besides this the study shall encompass different reports, books, law journals, statues of legislature of various countries, articles, publications and other material concerned within its ambit.
Chapter Plan

The study has been divided in six chapters.

In Introductory chapter the notion of cyber crime has been introduced. The chapter shall introduce the whole gamut of the cyber crime along with its amplitude and the challenge which it is posing before the international community since the operational dimension of the cyber crime is drastically different from the conventional crimes which can be perpetrated from a place far from the actual place of the commission of the crime. It shall also introduce the entire scheme of the research work.

Chapter II explores the conceptual notions of cyber crime. The term ‘cyber crime’ is a misnomer. This term has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. “Cyber crime may be said to those species, of which, is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime”. Cybercrimes are crimes of the digital age. They are bloodless, non-violent types of crime which are committed by computer literate persons whose way and method of committing the crime is highly sophisticated and technical.

This chapter briefly introduces the novel topics of cyber crimes, traces the crime concept in the primitive society and its journey to the present day information society. It gives a brief sketch of the history of the Internet, thereby setting the backdrop in which cyber crimes are committed. It also discuss how the concept of criminal liability of yesterday has undergone a transformation in the internet age and how the basic elements of crime, namely, the actus reus and the mens rea are interwoven in the cybercrime. It also deals with history of cyber crimes, cyber crime vis-a-vis conventional crime, aspects and impacts of cyber
crime and theories of criminal behavior in cyberspace. The chapter also chalks out the typology and conceptualization of cybercrimes by highlighting the difficulties in defining elusive crimes.

Chapter III deals with international scenario of cyber laws. This chapter shall trace and analyze the cyber laws of some prominent countries to combat cyber crimes. Besides this the chapter shall also deal with the International instruments concluded under the auspices of the United Nations to combat cyber crime since the crime has the international ramifications. The object of the chapter shall also be to explore whether there is any uniformity in the laws of different countries to curb the menace of the crime for it involves the problem of transboundary jurisdictional issues.

Chapter IV deals with Indian law regime to combat Cyber Crimes. This chapter shall deal with the statutory law foundation in India to combat cyber crimes. The Information Technology Act, 2000 is by the very fact based on the Model law on Electronic Commerce as adopted by the U. N. General Assembly. The Information Technology Act, 2000 has for the first time brought cyber crime, punishment and procedure for probing it within a legal framework. This is a comprehensive enactment both on e-commerce as well as cyber crimes. Chapter XI of the Act provides for some of specified offences restricted to tampering with computer source documents, hacking computer system, and publishing of cyber porn materials. The chapter highlights and analyses the recent amendments made in 2008 which can go a long way checking cybercrimes and evaluating the changes and making valuable recommendations in the field of cybercrimes. Amendments of the statutory provisions of the Indian Penal Code, 1860 Information Technology Act, 2000, The Indian Evidence Act, 1872, The Banker’s
Book Evidence Act, 1891, The Reserve Bank of India Act, 1934 have been also discussed in this chapter.

Information Technology Act, 2000 is though landmark first step and became mile-stone in the technological growth of the nation; however the existing law is not sufficed. Many issues in cyber crime and many crimes are still left uncovered. This chapter shall examine critically the efficacy of the cyber laws in India and it shall also be examined as to how far the existing law regime of cyber laws is effective enough to combat the rising trends of the crime. It will further examine as to what are the lacunae that hamper the law regime in dealing with the crime effectively by exploring the inherent legislative deficiencies with which they are suffering from and how these inherent legislative shortcomings can be done away with in order to make the law regime of cyber crime efficient and effective to deal with the expanding tentacles of the crime.

Chapter V explores the Judicial Response on Cyber Crimes. In this chapter the attempt of the researcher will be to trace and analyze the judicial pronouncements of courts of some prominent countries including the judicial response of the Indian judiciary to cope with the ever increasing menace of cyber crime. In this chapter the an attempt shall also be made to find out the judicial trends and propositions to curb the crime and whether there is a uniform approach of the different judicial systems of the world over in combating the crime since the crime is not confined within the municipal boundaries of a particular legal system.

Dr. L. Prakash case on cyber crime is very significant where the Court convicted the accused under section 67 of the Information Technology Act, 2000. The accused was arrested by Chennai police for making cyber pornographic images of his clients forcefully. In Mr. Jayesh S. Thakkar v. State of Maharashtra, the petitioner wrote a letter dated 29th
May 2001 to the Hon’ble Chief Justice of Bombay High Court about a pornographic site on the internet, and this letter was *suo motu* treated as writ petition.

Chapter VI deals with conclusion and suggestions. This chapter shall conclude the research work with the suggestions as to how the law regime can be revamped and made effective to deal with the ever expanding contours of the cyber crime because the nature and amplitude of the crime is not static in view of the development in the computer technology. Moreover, the law dealing with cyber crime has to keep pace with the perpetual change in the perpetration and *modus operandi* of the crime. Therefore, the need of the hour is to amend and adapt the laws in tune with the growing contours of the crime and to ensure that there should not be any gap between the letter of law and its implementation.

***

Estelar