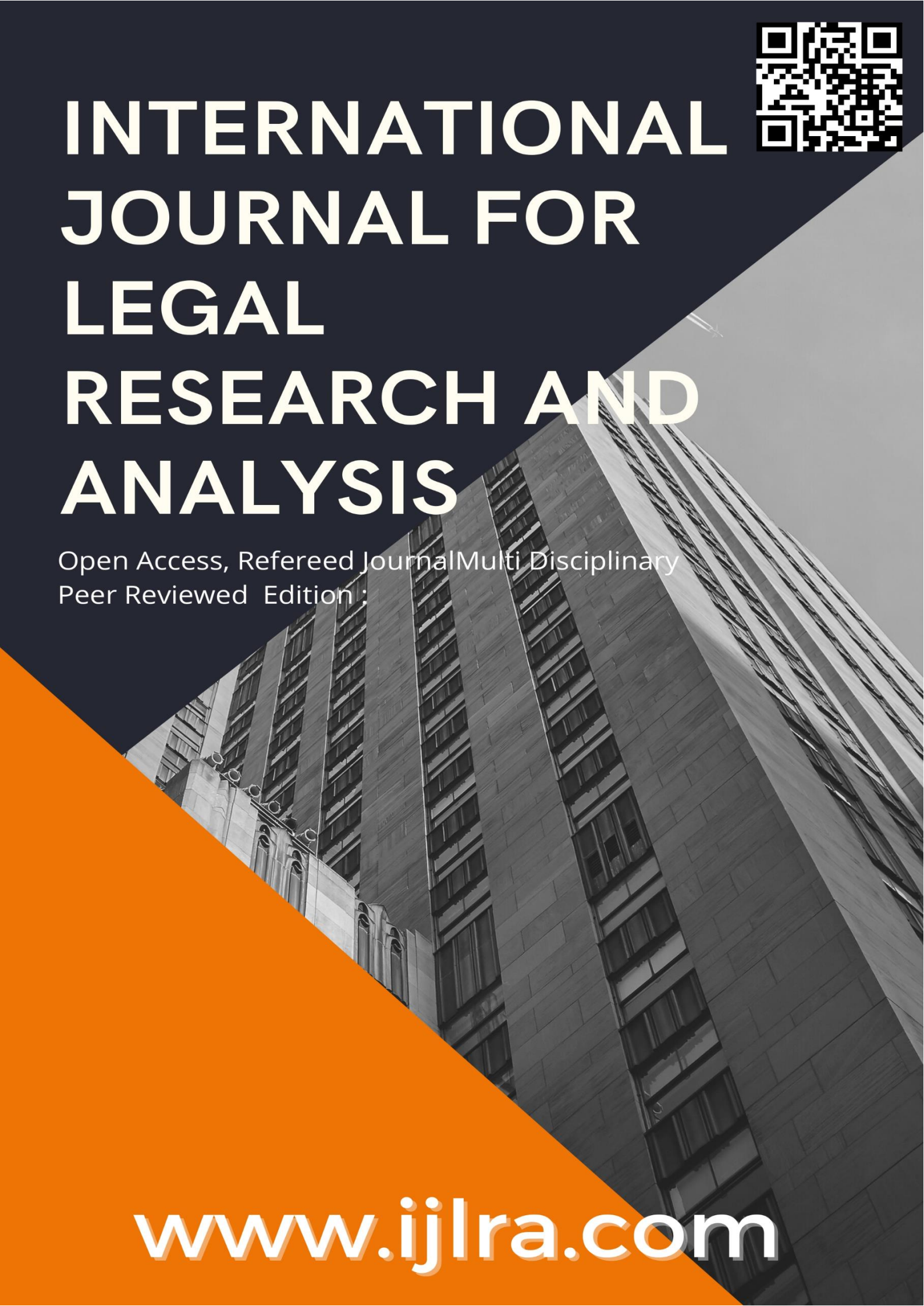
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :



www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

 ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

CYBER FRAUD IN RELATION WITH CYBER CRIME: A CRITICAL STUDY

AUTHORED BY - ISHAAN MALHOTRA

CHAPTER-I

INTRODUCTION

"Technology is a queer thing. It brings you great gift with one hand, and it stabs you in the back with the other"

- Carrie P. Snow

Human being is a social animal, the inherent nature of human beingis that , he needs personal safety, it includes security of life, liberty and property, is of utmost important to any individual. Maintenance of peace and order is need of everydeveloped society. It is possible only in state where the penal law is strong and effective and enough to deal with every situation. The society and its needs changes with the time, therefore the criminal law is required as per the situation. Thus, the prime object of Criminal law is the protection of public by the maintenance of law and order in every situation even in the information technology age.

Information Technology has brought a drastic change in the human life. Human intelligence has advances the life as easy way of communication, commerce, business and the banking also. The progress of civilization, as evidenced by the ever- changing information technology, easily accessible by use of computers was, no doubt put to use for improvement in living standard of human being. Information technology made improvements in every aspect of human life as like education, industry, commerce, governance, personal life style and social life around the world.

The information technology is very useful to the human life, which has made an impact

 ISSN: 2582-6433

on the social structure of the society. Especially the Indian culture is quite different but the information technology has connected the people. The social cites makes the platform to the nonprofessional to share their view, but along with the goodimpacts of it, certain adverse effect can be seen by the information technology. The privacy is going to violate by the cyber criminals, it create certain new mode to commit the existing crime, when the cyber space is going to be used for committing the crime.

Development changes the life style of human being but the human nature did not change. Human ingenuity has also use the technology for committing technology. Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "*a legal wrong that can be followed by criminal proceedings which may result into punishment."* The hallmark of criminality is that, it is breach of the criminal law. Asper Lord Atkin "*the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences".* A crime may said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cybercrime may be said to be those species, of which, genus is the conventional crime, and whereeither the computer is an object or subject of the conduct constituting crime." "*Any criminal activity that uses a computer either as an instrumentality, target or a meansfor perpetuating further crimes comes within the ambit of cyber crime".*

Cyber crime is an evil having its origin in the growing dependence oncomputersin modern life. In a day and age when computers are running everything from microwave ovens and refrigerators to nuclear power plants, cyber crime has assumed rather sinister implications. The evil of cyber crime is product of the technology but the basic nature of human being is the same and one. Therefore,the technology is the easy way to perform the act, which is against the law. The term cyber space is new. However, it creates the new modes operands forcommitting the crime or an illegal act by using the means of computer.

 ISSN: 2582-6433

The internet is a technical development gives us all opportunity toact as global community. Internet and electronic based treading affect all aspects of business. The information technology revolution is creating newbusiness and forgoing old one to either change or die. The traditional legal systems have a great difficulty in keeping peace with the rapid growth of the internet and its impact throughout the world. Telephone (though invented by Bell) it gives easy way of communication, which is more effective than the conventional form of communication. An internet or network of computers can operate without the constraints of space, state borders etc.

Cyber crime, which ramped in society in the recent years, the main cause is the easy access to the internet. By using the computer and internet, the person can commits the crime as like fraud, forgery, stealing the important data, pornography andrelated offences, which are nothing, but relating to the offences outraging the modestyof the woman. These offences recognize as a cyber crime but they are conventional crime only the tools are change. The Indian legal system has enacted the Information Technology Act 2000 and Information Technology Amendment Act. 2008, which recognized as a cyber law in India. However, the provisions, which are provided in the said act, are more concern with the business and less with the cyber crime.

Cyber crime is not different from the conventional crime. However, the tool hasbeen changed so it requires different tools for investigation. The basic intentionbehind the cyber crime is nothing but wrongful gain or wrongful loss or it may result in defraud someone, which is the base of the conventional crime as like the theft andcriminal misappropriation or fraud. Therefore, the cyber crime is not different from the conventional crime and subject to the regular criminal law of India.

The state in present era is welfare state, its first and foremost duty is to maintain peace and security. Effective criminal law is required to maintain the peaceand security. So for as the Indian Legal system is concern Indian penal Code is universal criminal law, which almost covers the crime, relating to all aspect. Apart from this, the various special laws are enacted considering the need by the Indian legal system. The Indian

 ISSN: 2582-6433

Penal code cover all the crimesas contended the conventional crime, and for the execution of this law, effective investigation is required, and therefore the Criminal procedure code[1] deals with the investigation andpowers to investigate. Execution of criminal lawis much more depends on the effective investigation.

The investigation of conventional crime as like theft, extortion, Criminal misappropriation, cheating is subject to the conventional procedure of investigation, the object of these all offences is nothing but the wrongful gain or wrongful loss. Forthis, object the criminal's tries to use different way to commit the crime. The crop agencies must be acquainted with different ways to commit the crime, otherwise the investigation hamper and the effect of criminal law will lack.

The criminals may always change the way to commit the crimes, though the object is similar, and therefore, it is not require enacting the special laws for those crimes. The cyber crime, known as the crime of 21st century, but the object of the cyber criminals, is nothing but wrongful gain or wrongful loss, or in certain cases withintention to devaluate the things or defame. Only they use different tools as like computer, internet.

The criminals may always change the way to commit the crimes, though the object is similar, and therefore, it is not require enacting the special laws for those crimes. The cyber crime, known as the crime of 21st century, but the object of the cyber criminals, is nothing but wrongful gain or wrongful loss, orin certain cases withintention to devaluate the things or defame. Only they use different tools as like computer, internet. Therefore, the investigative machineries require expert knowledge.

Aims And Objects:

The law changes from time to time. The criminal law of India hasalso developed with the changing of the time. The law is subject to the

[1] Guide to cyber Laws, Rodney D. Ryder,(2003) Wadhwa Nagpur, Page 2.

 ISSN: 2582-6433

changing situation of the society. Recently the amendment takes place in the Indian Penal Code in 2013,which drastically change the definition of the certain crime. Somewhere the provisions that is suitable to prevent the crime, which isgoing to be committed by using the technology, such as the Indian Penal Code sec 354(D) which deals with theStalking.

The research intends to do comparative study of the cyber crime and Indian criminal law. Whether conventional criminal law having sufficient provision to control and prohibit the cyber and new technical crime, Indian Penal Code is well recognizes universal code, which cover almost all kinds of crime and criminal acts, then which are the provision in Indian Penal code cover the aspect of the cyber crime. What is the relation of cyber crime and criminal law of India, is it needs certain amendment along with the Information Technology Act.

Cyber crime is technical crime it need not require other aspect of crime as like the conventional, the culprit can commit such crime from any place at any time. Dueto this aspect whether the present criminal law of India including the procedural andsubstantive law is sufficient to curb and control the cyber crime. However, so far the investigation whether the present laws are sufficient or certain special investigation machinery is require that is object of the research. It is intend to find out the presentlaws and it utility to controlthe cyber crime as well as to see the nexus between the conventional criminal law and Cyber law and make the comparative study.

Following are the objective of research:

1. To observe the provision of Indian criminal law and the relevant provisionswhich cover the offences like cyber crimes.

2. To make the study of cyber law including I T Act and the relevantPenalprovisions pertaining to cyber crime.

3. To make the comparative study of conventional Criminal law of Indianandcyber crime and laws relating to cyber crime

 ISSN: 2582-6433

To find out the shortcoming of the laws pertaining to cyber

 ISSN: 2582-6433

crime including the procedural laws i.e. The Code of Criminal Procedure andIndian Evidence Act.

Significance of Topic of Research:

Carrie P. Snow rightly said that the technology gives a wonderful gift to you by one hand and stop you by another hands. The present criminal law is in developedstage but the law behaves like a Hindu traditional wife, which is behind the seven steps from the technology. The technology developed in such a way that it now essential part of the life and therefore the present law is facing various challenges.

Crime and criminal law is not statistic, it changes from place to place and time to time, but there are certain crimes, which are as it is but the way of committing it has drastically undergone change. Due to the changing facets of the society, the lawsalso require to change its facets.

Along with the unique opportunities, the internet offers it is also poses new and significant ways to do the cyber crime. Most existing laws and enforcement system designed to address fraudulent and deceptive commercial practices. The current laws and systems are therefore not always adequate to control the cyber crime. Another challenge is the diverse legal system worldwide, with different laws enforcement procedure and role for judicial authority and varying reliance on Civil Criminal and cyber laws.

The concept of cyber crime is product of internet society, the cyber crimes aresubject of the conventional crime but the modus operandi is new that's why the conventional criminal law are insufficient to probe it. Therefore,it requires the new themes to control the cyber crime.

In Indian legal system the conventional investigation machinery investigate the cyber crime, The I T Act has introduce some special bureau for investigation but italso works as like conventional crop agency.

Literature Review:

The development of every country is depends on the legal system of the state. Now a day, Criminal law has well developed, but the need and situations are alwayschanges

 ISSN: 2582-6433

in every country, so it is necessary to the country to develop the criminal law as per the situation. In 20th century, the World is called as a cyber world. The information technology is very much developedin present days. Internet is the essential part of the human beings life today. Internet make the world a globe, whichbring with it the misuse of the computer means the cyber crime. Cyber crime is inevitable but the highly educated person generally commits it. To prevent the cybercrime every country made cyber laws. Indian legal system also enacted the Information Technology Act 2000. However, it is more business law than the cyber law.

The present research is undertaken by researcher to analysis the cyber law, its investigation, and its comparative study with conventional crime. The researcher adopted doctrinal research methodology and hence gone through primary and secondary data to complete this research work.

1. Indian Penal Code- Ratanlal & Dhirajlal Wadhwa, Publication Nagpur 29th edition 2003

This book is well known in criminal law, the author is renowned writer in criminal law. The first chapter of the book deals title and extent, in this chapter the author rightly discussed the concept of crime and the development of the criminal law in India. This book discussed all the provisionsof penal law. The author tries to describe the each section along with the landmark judgments, which help the reader to understand the interpretation of the section. This book helps the researcher to understand the criminal law in Indianlegal system. It is useful to see the content of the conventional crime and that can be compared with the cyber crime.

2. PSA Piliai's Criminal Law – Dr. K.I. Vibhute

The author of this book is well known in research and former head of the Law Department of Pune University, the book deals with the conventional criminal law or Indian Penal code. All the offences are discussed in detail along with its ingredients and the commentary in the section gives the central idea ofthe said section. While reading the

 ISSN: 2582-6433

section from the book, we can easily understand the nature of the sectionsobject of the lawmaker. The research work of the book regarding the references guides the new researcher, how to refer the books and the case laws while writing.

3. Criminal Law: cases and material – K. D. Gaur

This book of criminal law deals with the principles of criminal law. To understand the principles of criminal law, it must be understood the basic thing on which criminal law is based, which is necessary to understand. The author of this book is well known writer in the subject of criminal law. The book deals with criminal law along with its principles. The title itself suggests that the principles of criminal law are discussed along with the landmark cases. Generally, the codified laws are not having much impact of the case laws. Because the criminal must be specific otherwise it will be just chaos, the author emphasis this thing.

While discussing the Indian Penal code, the author discusses the basicprinciples behind the section, in simple the base of that section. The author discussedthe criminal law in such a manner, that the base of criminal law can be studies from this book. Though the society changes time by time, it needs changes but the basic things of criminal law are almost similar.

4. Judicial Jurisdiction in transnational cyber space- Bimal Raut. New EraLaw Publication, Delhi (2004)

This book is best research in the era of the cyber law. This is theresearch on the problem of the jurisdiction in cyber crime. The peculiar characterof cyber crime itthat, it can be committed from any corner of the world, which affect to a person who is in another corner of the world. Now the problem of jurisdiction may arise, for talking legal action against that person which law can be applies. For this issue, the author has discussed all the relevant laws, section and the international convention. Inconventional crime and criminal law, the land laws regulate the crime and having power to control and curb it. However, in cyber crime the problem of jurisdictions arises. This book help to

 ISSN: 2582-6433

understand the problem of jurisdiction in cyber crime and thesolution which international community has tries to provide is discussed by the author.

The author discuss the cyber law from all angle, its inanition, how business lawturn in towards the information technology, then historical development of cyber crime law , international perspective of cyber crime and cyber law. It discuss making of Information and Technology Act. The book deals with the first cyber law in India, which enacted in 2000. The book is useful to the researcher to get the basic concept of cyber crime and cyber law.

5. Guide to Cyber Law – Rodney D. Ryder (second Edition 2003) Wadhwa Publication Nagpur

This book is the complete guide on the cyber crime. 20th century is the century of information technology. Now we are living in cyber world. Initially this technology is going to use for commercial purpose, but now a daya common person is connected to the cyber world for his regular life, therefore the cyber law is also part of the life of common man. The book deals with the entire development of the cyberspace and cyber world. The author discussed how the international community has started to recognize the online communication in the business transaction and the regulation of the transaction.

How the international community has meet on the issue of this internet transaction, the first International convention on the online transaction has discussedby the author. The author discussed the International perspective of cyber law, then all the important convention, which takes place on the issue of internet. Then how the UNCITRAL model of the law on the internet is also discusses. It discusses making of the Information Technology Act 2000 and the important provisions of it along with the commentary. The book is useful to the researchers.

6. Cyber law and crime – Barkha U Ram Mohan (Asia Law House)

 ISSN: 2582-6433

Hyd.3rd edition.2011

The author of the book is a practicing advocate in A. P. High Court. The author discusses the cyber law and crime in view of Information Technology Act. While discussing the cyber crime the author discuss the process of search and seizer. In simple, the book deals with the procedural aspect of investigation of the cyber crime and the relevant provision of the law. This kind of books helps the research to deals with the practical problem in the cyber crime investigation andthe difficulty inthe cyber crime investigation.

7. Cyber crime –Law &Policy and perspectives- Dr. Mrs.K.Sita Manikyam (Hind Law House) 2009 Edition

This book is useful to understand the relation of technology and law.The book is contented in 10th part, the first part deals with the technology and the use of technology in the life of common people. Then the author discusseshow the misuse of technology affects the right of individual as like the right of privacy. Nowinterfering in the privacy of person by using the technology of computer is amount tothe cyber crime. In next part of the book, the author discussed the conceptual analysis of the cyber crime.

The book deals with specific cyber crime, and investigation of cyber crime. Cyber crime investigation is now a complex issue before the investigation machinerydue to lack of knowledge. The author gives the processes and the solutions on the problem regarding the investigation. Lastly, the author discussed the problem of jurisdiction of the cyber crime; therefore, the book is useful which gives the central idea of cyber crime and policy and perspective of the cyber crime.

8. Criminal Procedure Code – S.C. Sarkar (Indian Law House)New Delhi8th edi2004.

This book deals with the procedural aspect in the criminal law. Cyber crime is subject of state and the proper investigation needs to protect the society from thesaid crimes.

 ISSN: 2582-6433

The Information technology Act is quite business law and theoffences are subject to general investigation by the same agencies. This book deals with the procedural aspect in conventional crime so it is useful to the researcher.

9. ***Cyber Law Cyber Crime Internet And E-Commerce- Prof. Vimlendu Tayal , Bharat Law Publication, Jaipur. First Pub. 2011***

This book is the collection of the various articles by the expert onthe cyber law and related subject. It is great collection on the cyber law and cyber crime. This book provides the information regarding the jurisdiction and related concept of the cyber crime. Apart from this, the different author discusses the cyber crime and the cyber law in different facets. This helps the researcher to understand the concept of

the cyber crime and the practical problems. It discusses the Information TechnologyAct 2000 and the related issue.

Hypothesis:

Indian Criminal law is now well developed; so for as investigation of crime is concern, various new methods are going to be followed by the investigation machinery. However, in recent era due to globalization and drastic development in the Information and Technology and internet the new challenges are come before the legal system that is of cyber crime. Internet and its easy access is the main reason behind the cyber crime. In 1978 the concept of internet was emerge and in 1989, thefoundation of World Wide Web (WWW) takes place. Internet user has significantly increased over the past few years in India. When internet was first developed, the originators never thought about that internet could transform into a useful communication tool and could be misuse for criminal activities and which require monitoring.

Use of Internet to commit the crime is punishable by the criminal law. Cybercrime is nothing but the subject of conventional criminal law but what development takes place regarding the Internet, which leads to cyber crime but the criminal law hasnot amended in such a way that is why the problemof cyber crime is increase and need

 ISSN: 2582-6433

certain appropriate measures to curb it.

So for the study of criminal law and cyber crime following hypothesis

- Cyber crime is subject matter of the conventional criminal law.
- Cyber crime and conventional crime are not different but the way of committing the crime in cyber crime is different
- Cyber crime is expansion of the conventional crime, to control it certain newpolicies are required.
- There is close relation between cyber law and criminal law
- Cyber crimes more spread due to lacunas in the investigation process
- New substantive laws are not required but procedural laws must be amended and expert investigation machinery and adjudicatory authority must be appoint for controlling the cyber crime.
- To control cyber crime special investigation force must be need and the present investigation authority need the assistant of the expert in law and computer.

Research Methodology:

Considering the aims and objectives of the research the methodologyis adopted literature review and research through accessing hard copy andelectronic libraries has the main source of collection of information and data. Primary source of materials are the present statute for the crime and the cyber law. For the research thelaws regarding cyber crime and conventional crime in India and Its amendment is themain source.

The other sources are concerns that are nothing but Indian Apex courts Judgment and the High court judgment are also the source of the research. The courtsview regarding the cyber crime has to see. The main part of research is to see the similarities and differences in the conventional criminal law and cyber crime by analyzing the Statute of Indian Legal System.

The data collected from the different sources has been compared, which providesthe results in all means for the research subject.

 ISSN: 2582-6433

CHAPTER-II

THE LAW RELATING TO CYBER CRIME IN INDIA

The concept of crime is not a modern one but it has been existing from timeimmemorial. However, time to time, the concept and nature of crimes have changed. In addition, the definition of crimes has been changed accordingly. In the era of 20th century and with the advent of computer, the criminals have changed the mode of committing the crimes from conventional methods to computer based methods. The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which isthought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China.[2] Indian legalsystem is now in a developed stage. Indian Legal system is enacting the law along with the changing situation. As Prof. Allen has rightly contented that, the law is not only deals with command but is something more. This view shows that the role of lawis broader than the command. This role of law is more relevant in the present situation. Thecriminal law closely connected with the each member of the society. In the ageof information technology, cyber law is need of hours. The cyber law means the law relating to the cyber crime.

[2] http://hubpages.com/hub/Cyber-Crime last access on dated APRIL 2023 at 8.00 am.

 ISSN: 2582-6433

A person seating in any corner of the world can communicate to other person without disclosing his identity. Due to this nature of internet, it raised various challenges not only to the government but also to the trade and individual of the entireworld. Therefore, the legal system awakens and required to make certain legislations to protect the interest of the entire society. Therefore, this new branch of law is emerged, because the conventional procedure to prevent the crime is useless for offences committed through the computer or internet. The rules and regulation, whichdeals with the cyber space internet and its regulation, are subject matter of the cyber laws.

Until 1999, India did not have any legislation to govern the cyber space.However, due to the development in communication and e-commerce, internet makesimpact on the cyber world. This compel to the legal system to enact the rules to govern the cyber space. Due to the huge use of internet, some alert nations of the world formulate the policy. India is one of the nations among them. Indian legal system introduced certain enactment and amendment in criminal laws, which can called a cyber law. However, cyber crime is not different than the conventional crime, but it need certain new policies to regulate and control the cyber world.

2.1 Concept of Cyber crime

The term cyber crime is nowhere defined, this concept is vary because the crime which is going to committed by using any means of communication or internetcan be called as a cyber crime. The misuse of the computer or the internet is not specific therefore, it is not possible to define the cyber crime specifically. To understand the concept of cyber crime, it is necessary to see the concept of crime, which is, attach with the computer and the internet. The concept of cyber crime is not radical different from the concept of conventional crime. Both include the conduct whether act or omission which causes breach of rules of law and counterbalance by the state[3].

In initial period, the crime is quite different and depends on the will of the sovereign authority. Now a days the crime is a social and political phenomenon and it is as old as the human society Along with the development, the concept of the crime is legal

 ISSN: 2582-6433

and back by sanction. Now crime means a legal wrong. Initially it is somewhere the religions wrong when the religious institutions were powerful. Therewere no difference between sin and crime. However, alongwith the development of State, the concept of sin was diluted and the sin or wrongful act term in to a wrongfulact. This wrongful act now turns in to the concept of crime or offence. According to Granville Williams, crime or offenceis a legal wrong that can be followed by criminal proceeding, which may result into punishment. The basic thing in criminality is that, it is a violation of criminal law.

The cyber crime, which is the new term, the cyber, is also newly generated term. When by using the internet, anything going to be done in that cyber space, this is not found in physically existence that is called a cyber space. When anyone uses this cyber space to committee the crime, it is called a cyber crime. Cyber crime is not new but it is as like the conventional crime .Basicallythe crime means any act, which is going to commit against the society and create an alarm in the mind of society, or create a fear in society. So cyber crime means when any person by using the internet or computer performs the criminal activity as provided in any criminal law, that crimecan be called as a cyber crime. When the word cyber comes, it deals always with thecomputer orany network. When this computer or internet is used to commit a crime, it is cyber crime. In cyber crime computer is an instrument to commit the crime or itmay be a target.

[3] Cyber crime- Law & policy perspectives, Dr. Mrs. K. Sita Manikyam (APRIL 23) Hind Law House, Pune.Page 40.

In the present era of rapid growth, information technology is encompassing all lifestyles all over the world. These technological developments made the transitionfor paper to

 ISSN: 2582-6433

paperless transaction possible. We are now creating new standards of speed,efficiency and , accuracy in communication, which has become key tools for boostinginnovations, creativity and increasing overall productivity. Computers are extensivelyused in the storage of confidential data of political, social and economic or personal nature, which are of immense benefit to the society. The use of Computers is increasingly spreading, and more and more users are connecting to the internet. Due to this situation it is an easy access to the internet and the computer. Therefore, the criminals started to misuse the computer or internet for the criminal activates. The internet is a source where anybody can easily access, manipulate and destroy other information, this activities are nothing but the cyber crime.

A generalized definition of cyber crime may be "unlawful act wherein the computer is either tool or target or both, the computer may be used as a tool in financial crime or sale of the any illegal articles. The computer may be the target when someone tries to unauthorized access to the computer or any personal data; thiskind of misuse of the computer or the computer networks is called cyber crime.

There is apparently no distinction between cyber crime and conventional crime. However, on a deep introspection we may say that there exists a fine line of demarcation in the involvement of the medium in case of cyber crime. Thesine que non for cyber crime is that there should be an involvement, at any stage of the virtual cyber medium. Means the cyber crime is subject to the cyber space. Offences committed via Information technology are known ascyber crime. This information technology based on the cyber world, but computer does not subjected to commit cyber crimes. However, the computer hand in hand with the internet has gives birth to a new generation of crime. In such computer crimes, the role of human hand is less while the automated machines carry out the major activities. While the Internet is thewonder gift of science to humankind, at the same time it becomes a haven for criminals.

The cyber world is the non-physical and the boundary less. Although, thecomputer world may exist only in intangible form, it affects the physical and real environment.

 ISSN: 2582-6433

The shift of crime to intangibles has a staggering impact on society, both socially and economically. This Social and economical impact is all over the world because, due to internet and information technology, the world becomes a global village. The internet is not subject to any particular state, therefore, the cyber law and the cyber crime cannot be subject to any particular country or State. Therefore, it is necessary to see the global perspective of the cyber crime. Being an international subject all Nations has try to enact the laws regarding cyber crime and tries to define the concept , thought it is not possible to define the cyber crime, but itis necessary to define the cyber crime for the execution of the cyber laws.

2.1.1 Definitions

The cyber crime is worldwide problem so various authority, national and international level tries to define the term cyber crime. Following are certain important definitions. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet. The Encyclopedia Britannica defines 'cyber crime' as anycrime that is committed by means of special knowledge or expert use of computer technology. So what exactly Cyber Crime is. Cyber Crime could reasonably include awide variety of criminal offences and activities.

The words cyber crime and computer crime are use inter changeably in common parlance. The word computer crimes has wider ambit as it entails not only crimes committed on the internet but also offences committed in relation to or with the help of computers. Don B Parker distinguishes between the concepts of computer crime and cyber crime, and gives the definitions of the terms in the following words.

1. Computer crime: A crime in which the perpetrator uses special knowledge about computer technology.

2. Cyber Crime: A crime in which the perpetrator uses special knowledge of cyber space.

A computer crime defined by the U S department of Justice's "As an illegalact requiring knowledge of computer Technology for its perpetration, investigation

 ISSN: 2582-6433

orprosecution". However, the definition is not exhaustive as there are many acts, whichcan be called abusive activities concerning the computer but they are often not clearly illegal. Moreover, most of the cyber crimes are committed via internet but the definition has no reference to it.

Cyber crimes can be plainly define as " Crimes directed at a computer or computer system" But the complex nature of cyber crimes cannot be sufficiently expressed in such simple and limited term.[4]

The Organization for Economic Co-operation and Development (OECD) recommended the working definition of cyber crime "computer related crime is considered as any illegal, unethical or unauthorized behavior relating to the automaticprocessing and the transmission of data."

This definition is also cannot cover the border aspect of the real nature of the Cyber crime, while defining the cyber crime, it only cover the illegal activities pertaining to the data transmission. However, the cyber crime not only deals with thedata transmission, it includes every illegal activity via computer.

In 2001, The Council of Europe Convention defines cybercrime in Articles 2-10 in four different categories: 1) offences against the confidentiality, integrity and availability of computer data and systems; 2) computer- related offences; 3)

[4] Cybercrime: Talat Fatima, (2011) Eastern Book Company, Lucknow. Page 89.

 ISSN: 2582-6433

content- related offence; 4) offences related to infringements of copyright and related rights.[5]

This is not definition but it explanation of the cyber crime, which cover four limb in the illegal use of the computer and the internet. The council has broadly coverall the activities in which the privacy of some once going too violated byusing the computer or related network. It also covers the integrity. It use the computer related crime means it use same word which cannot give any precise meaning .This definitionis very broader in sense cannot give any precise meaningof the term cyber crime.

On all above definition, the conclusion can be drawn, that the cyber crime is much border and wide term, yet the correct definition of this term is not available. There are various cyber laws enacted by the various Nation, but any nation cannot provide the unities Cyber Law that has cover the completeconcept of cyber crime. The countries have to enact the multiple laws to coverthe misuse of the computer andrelated crime.

Cyber Crime may be defined as the "act of creating, distributing, altering, stealing, misusing, and destroying information through the computer manipulation of cyber space; without the use of physical force and against the will or the interests of the victim"

This definition has specifically content the nature of cyber crime, as the cyber crime is going to commit in the cyber space. Thus the basic thing in the cybercrime that it ever requires the physical force. Whenever the person misuses the cyber spaceto commit, any illegal act that can be called as a cyber crime.

The information Technology bill, 1999 defines the cyber crime as, "Whoever knowingly or intentionally council, destroy, or alter or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document use

[5] Cyber Crime and National Security: The Role of The Penal and Procedural Law by Laura Ani

 ISSN: 2582-6433

for a computer, computer program, computer system, or computer network, when computer source code is require to be kept or maintain by law the time being in force shall bepunishable with a fine which may extent up to rupees two lakhsor with imprisonment up to three years, or with both."[6]

Some of the commonly spelt out definitions of cyber crime are:

1. A criminal activity that involve unlawful access to or utilization of computer system.
2. Any illegal action in which a computer is use as a tool or object of a crime; inother words, any crime, the means or purpose of which is to influence the functions of a computer
3. Any incidents associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention madeor could havemade a gain.
4. Any violation of the law in which computer is a target of or the means for committing crime.
5. Any activity, which involves the unauthorized and unlawful accessto or utilization of computer system or network in order to tamper with the help of computers and the internet, can broadly be called as cyber crime.

On these spelt, it shows the concept of the cyber crime. However, anyauthority has not provided the definition or even Act has not provided the definition of the cyber crime.

merely a computer. Therefore, the mere computer or the internet is not subject of thecyber crime, but both things are part of the cyber crime. Therefore it is difficult to define the cyber crime .Basic reason behind it is that, it is not different that the conventional crime and it cannot be subject to any particular way of misusing of computer or the internet.

2.1.2 Essentials of Cyber crime:

[6] http://www.nalsarpro.org/CL/Modules/Module4/Chapter-1.pdf last access on dated 04/4/14 at 8.00pm.

 ISSN: 2582-6433

The term cyber crime cannot define due to the critical nature of it, because it involves the crime relating to computer and computer techniques.[36] Therefore, it has not any specific ingredients different from conventional crime apart from thetechniques. Because development of technology create new way to commit the crimecalled the cyber crime has emerged which is radically different from the conventional crime. This crime is the ill effect of the development of internet regime. In view of the peculiar nature and repercussions of cyber crime, its characteristics are altogether different from that of a conventional crime. The most striking features of cyber crimesare that they are relatively easy to commit, difficult to detect and even harder to proved. This is the reason as to why these crimes have been characterize as low risk high rewarding ventures for the cyber criminals who with basic computer knowledgeand skill can easily destroy valuable database causing huge loss or damage to the affected victims of the crime.[7]

Many a times even the victim affected by cyber crime is unaware of itsoccurrence because of lack of adequate skill and know how in handling the computersystem.

with the routine working system and has a good understanding of the loopholesand availability of opportunities to commit the cyber crime without leaving anytrace forpossible detection. Apart from the employees who are unhappy with their employeesfor one reason or the other may tend to target the employees computer system to takerevenge similarly, business rivals may also try to have unauthorized access to system of their computing counterpart and steal away confidential secret data from his computer system for personal gain. [8]

Cyber crimes have been characterized as high tech offences because they are committed by the abuse of computer networks and telecommunication technology. The range of such crime is wide enough to affect the socio-

[7] tecindia.co.in/navneet/navneet-cyberlaw/MIR-012-B2 last accesson

[8] U.N. Congress on prevention of crime & treatment of offenders held in viagna on April 2023

 ISSN: 2582-6433

economic and the legal rights of the people. Through, the use of computer network system in itself is legal butthe illegal actions in using the networks asa medium are deemed illegal andpunishable under the criminal law or the cyber law or both. Like any other cybercrime the hi-tech cyber crime committed through the computer telecommunication networks has the following

1. The perpetrators as well as the victim both remain anonymous and difficult to be identified.
2. Many unspecified potential customers are used through they may be far awayfrom the place of crime.
3. Evidence against the crime is easy to erase thus rendering the helpless.

Being, a social animal, whose nature and need is to communicate with each other, connected with this technology. Now a day the entire life of human being is depend on the information technology.

Computer is a product of the 20th century. It has drastically changed the modes of information technology. Along with the utility of the computer, whenever any techniques bring easiness in the life of human being, it brings similar risk with it. Thecomputer and this internet bring cyber crime with it. Thus, cyber crime are unknownto the legal world prior to the birth to the internet and includes not only acts which areemployed to commit the traditional crime using the net but also those crime which are committed thoroughly and exclusively using the internet. Though certain cyber crimes are thoroughly committed by using the net, that also nothing but somewhere attach to the conventional crime, thereforeit is difficult to define the cyber crime.

The United Nation highlighted the problem of definition in its manual on the prevention and control of computer- related crime, stating that although there is consensus among experts, these definitions have been functional and hence too specific. A similar problem was expressed by the Council of Europe, the committee on crime problem decided to leave out any definition of high tech crime in the Convention on Cyber (2001), allowing individual jurisdiction to apply their own definition based on their specific body of law.

 ISSN: 2582-6433

It is however interesting to note that the IT Act 2000 too omits to define cyber crime or computer crime. This Indian situation, though the Indian legal system enacted cyber law very recently in year 2000. Even themajor cyber laws of the US and UK do not content a definition of cyber crime. However, the taxonomy ofthese elusive crimes would give a circumvention and exhaustive comprehension of cyber crime. In India, the recent amendment in the IT Act, 2008 has used the term' "computer related offences" whereby a good number of cyber crime have been added to the list of crimes already existing.

Thus, the cyber crime cannot define due to these problems, and it is agreed bythe national or international authorities. On the minute observation of all the cyber crime policies of the entire countries, Cyber crimes are generally covered in conventional crime, as like offences against property, offence against privacy, against security or intellectual right. Therefore, it is not necessary to define cyber crime specifically, being part and parcel of the conventional crime.

2.1.3 Reasons for Cyber crime

Crime is a social phenomenon and there are various reason behind the crime. Criminologist had studied by giving different reason but the entire criminologistgives different reason. Cyber crime is creation of the technology and the technology makesthe life of human being easy, therefore every one attracted towards this technology without sufficient knowledge. This technology is having various special feature due to which is gives opportunity to the misuse the technology for commission of crime. AsProf. H. L .A. Hart in his classic work entitled, "The concept of law"[9] has stated that, human beings are valuable to unlawful acts which are crimes and therefore, rules of law are required to protect them against such acts. Applying the same analogy to cyber space, the

[9] Cyber Crimes: Law & Policy Perspectives, Dr.Mrs.K.Sita Manikyam , (2009)Hind Law House, Pune Page 41.

 ISSN: 2582-6433

computer systems despite being hi-tech devices are extremely vulnerable Computer is an electronic device which carries out its functions with the help of complex technology rather than manual actions of human beings. The greatest advantage of networking in the computer age is the wider access to information resources over a large and extensive medium More and more organizations are restoring to networks for providing easily accessible information to their employees customers and parties with which they deal.

Information dissemination through World Wide Web has created new resources for faster and cost effective easy access to information throughout the world. It has created new environment of e-mails, chats, down loads etc. However, wider access to information creates some problems like protecting and guarding any computer system against unauthorized use.

1) Wider access to information

Access where there is possibility of breach not due to human error but because of the complex technological manipulations. For a bank vault, which usually contains lakhs of rupees is well guarded against unauthorized access by miscreants as it is made up of very strong materials located in a reinforced zoom guarded by security personnel, secret information can be easily stolen by implementing logic bombs or key images in access codes. Similarly, the advanced voice records can easily fool biometric systems and frustrate all security measures.

2) Complexity of computer system

The computer work an operating systems and these operating systems in turnarecomposed of millions of codes. Human mind is fallible and it is possible that theremight be a lapse at any stage. The cyber criminals take under advantage of these lapses, lacunas and penetrate into computer system. Such criminals are called hackers who exploit the weaknesses in existing operating system andsecurity devices. Thus, hackers are the dreaded enemy of the internet and general network security and theyexploit the complexity of computer systems motivated by personal vengeance. Sabotage fraud, greed

 ISSN: 2582-6433

or malice against the victim.

3) Negligence of Network users

Negligence is closely related to human conduct, It is therefore quite probable that while protecting the computer system there might be any lapse or negligence on the part of the owner, thus user which may provide an opportunity for the cyber criminal to gain unauthorized or illegal access or control over the computers Interaction with the cross- section of computer users has shown that in their anxiety to put the computer software into regular operation. They allow the access control and security measures to take a back seat thus providing scope for cyber criminals to intrude and steal after or erase substantial data. This is particularly true with big organizations such as banks, corporations, government offices etc. which are equipped with high tech software systems for public access but leave if totally insecure and unguarded against information poachers or manipulators due to sheer negligence of their staff or employees.

4) Non- availability or loss of evidence

The traditional methods for producing storing transmitting and disseminatinginformation or records has now been replaced by the digital computer processing andnetwork technology. The real issue before law enforcement and investigating agenciesis how to procure and preserve evidence unlike traditional offences, it is very difficultto collect sufficient evidence of a cyber crime which could withstand judicial scrutiny to establish the guilt of the cyber accused beyond doubt. Anonymity that internet provides to the cyber criminals encourages him to indulge in criminal activity without leaving any evidence and even if some evidence is left it is hardly sufficient to convince the police that a criminal case can be registered against the perpetrator.

The inadequacy of traditional methods of evidence and crime investigation has necessities adoption of new techno-legal procedure called cyber forensics, which has broadly been classified as computer forensics and network forensics. The forensic experts play an important role in collecting and presenting admissible evidence electronic evidence, search and seizure of material evidence relevant to the cyber crime under investigation. But still these are certain grey areas which enable the cyber criminals to tamper with the evidence

 ISSN: 2582-6433

to mislead the investigating agencies.

5) Jurisdictional Uncertainty[10]

Cyber crimes cut across territorial borders which undermine the feasibility andlegitimacy of applying domestic laws which are normally based on geographical

[10] Conventional crime through computer e-book.

 ISSN: 2582-6433

or territorial jurisdiction, Cyber crimes are committed through cyberspace network inter

connectivity and therefore, they do not recognize geographical limitations because of their transnational in nature. There being no uniformity in law and procedure amongthe different nations for handling cyber criminals, jurisdictional conflict a serious problem for a nation to deal with the cyber offenders. In many cases,it so happens that create particular cyber activity is recognize as a crime in one country but it is notso in the other country where the criminal or the victim resides with the result the criminal easily escapes from prosecution.

In the absence of a single internationally recognized code of law and proceduregoverning cyber crimes the law enforcing authorities of individual countries findit extremely difficult to tackle cyber crimes and criminals while applying their territorial law. Briefly stated, reporting and conviction in cyber cases is far and few due to paucity of cyber jurisdiction of the country investigation or trying these offences and this uncertainty of law encourages the cyber criminals to continuetheir notorious activity unabated.

2.1.4 Types of Cyber Crime:

The cyber crime is generic term that can be use by various illegal activates where in computer or computer network is going to use. The computer crime and cyber crime are literally different but that cannot separate from each other by the legalsystem. Therefore, it is not easy to classify the cyber crime. There are various modesand manner by with the cyber crime can be committed. Even the traditional crime is going to be committed by using the computer or internet. The concept of crime is itself dynamic, and in case of cyber crime, it is more dynamic. Therefore, the cyber crime can be classified in various ways. It may classify on the use of computer or mode of using of computer in any crime. The role of computer in every cyber crime is different so it can classify on that basis also, it can classify on the basis of perpetrator. Role of computer means insider and outsider. However, the mode or role is not subject matter of criminal law but the result is more important, therefore on the basis of result ofillegal act, Thus the cyber crime can be classified on the basis of victims in the manner as following

2.1.4.1 Crime affecting Individual

 ISSN: 2582-6433

2.1.4.2 Crime affecting economy

2.1.4.3 Crime affecting national security

a) Crime affecting Individual

Cyber crime has started to take place by this kind. Maximum cyber crimes are commit which affect the individual. In this cyber crime, the victim is the user of the computer or someone used the computer by the name of the victim. The criminal getaccess to the computer or account of the other and uses the private access by violatingthe privacy right of the victim. The computer is a common and important source of preserving personal data or information. Internet andthe computer develop the techniques to restore the huge data of person in minimum time. Due to the capacity and the easy manner, this techniques is going to use in everywhere from school to hospital and business enterprises to governmental and nongovernmental banking alsomake use or abuse of it[11].

Internet and computer in business is call e-commerce. This e-commerce provides various speedy and less expensive procedures in the high- tech business. Thus e- commerce has removed the national boundaries without any problem. Due to this, lessexpensive process attracted the traders and businessperson to use this mode for transferring the huge amount of money. However, this process is also not without disadvantages.

The businessman and common man uses this technology to save their time, but criminals use the technology which is unknown to the general user of the internet and the technology is more sophisticated technology which is more

11 Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 48.

 ISSN: 2582-6433

easier way to commit the criminal activities. The criminal activity as like hacking and IP spoofingare the common offence, which are going to commit against the economy. Generally, the frauds are going to be committed by using internet. Software piracy is the common offence in a day, the object behind software piracy is nothing but to save the money. Cyber squatting is another mode to commit the cyber crime. The main object behind these offences is nothing but to gain wrongfully. This is new mode to commitconventional crime though, it is known as a cyber crime.

b) Crime affecting National Security:

When the illegal activity in the cyber space, that affect the society and nationat large are called cyber crime against the national security. Now a day the internet is going to be use for spreading the ideas. When such use is made by the terrorist organization to spread their ideology, it will threat the national security. Apart from this, there is also a major threat of terrorist attempting disrupt the telecommunicationand information technology apparatus itself.

This mode of the cyber crime threats the national and international perspective. Cyber terrorism is best example of this offence. Terrorists are using the recent information technology to formulate the plans, raise funds, create propaganda, andto communicate massage among themselves to execute a plan. [12] Cyber warfareis another mode to committee the cyber crime which affect the national security. Computer and internet is integral part of military strategies of various countries in theworld. By using the technology when one country collects the information of enemy country, it creates the threat to that country as well as the peace and security of theworld is going to be affected by this kind of activities.

The cyber crime is generic term that can be use by various illegal activates where in computer or computer network is going to use. The computer crime and cyber crime are literally different but that cannot separate from each

[12] Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 48.

 ISSN: 2582-6433

other by the legalsystem. Therefore, it is not easy to classify the cyber crime. There are various modesand manner by with the cyber crime can be committed. Even the traditional crime is going to be committed by using the computer or internet. The concept of crime is itself dynamic, and in case of cyber crime, itis more dynamic. Therefore, the cyber crime can be classified in various ways.It may classify on the use of computer or mode of using of computer in any crime. The role of computer in every cyber crime isdifferent so it can classify on that basis also, it can classify on the basis

2.1.5 Cyber Crime and Offences under Indian Penal Code

As the society changes, the concept of the crime develop along with the time and invented the cyber crime. as already mention that cyber crime is criminal act in which the computer or the network is either tool or target or both. In India, the criminal law means nothing but the Indian Penal Code, this the complete code which deals with all the offences, it dealing with all kinds of offences, though the concept of crime is new and technical, but the Indian Penal Code is still effective and covering all kinds of crime. Therefore this conventional criminal law is sufficient to deal withall kinds of crimes, whether this cyber crime or any other crime.

Indian legal system enacted Information Technology Act, 2000 with intent to regulate the e-business. That is purely a contractual law dealing with the commerce, but along with e-business, it provides certain provisions dealing with unauthorized use of the internet or unauthorized use of the computer. This misuse is called as a cyber crime in The Information Technology Act, 2000, which is India's cyber Law. The offences provided in this Act are already provided in Indian Penal Code in the variousprovision from the enactment of the Indian Penal Code.

After coming into force of the Information Technology Act, 2000 on 17th October,2000 appropriate provisions have been incorporated in the substantive criminal law of India. The substantive criminal Law of India means Indian Penal Code, because the various offences of this law are too much similar to the offences which are known cyber crime, only due to technology to commit that offences is

 ISSN: 2582-6433

quitedifferent therefore the amendments are require to bring that offences under the preview of this Code. The amendment insert certain new term in the Indian Penal Code only with intent to make effective implementation of provisions dealing with this offences which are going to commit by using the information technology.

The Information Technology Act, 2000 contains wide range of offences such as tempering with computer sources, sending offensive messages, violation of privacy; publishing obscene material etc. these all illegal activities are already recognized as an offence in Indian Penal Code. These similarities can discussin the following ways;

Similar offences also fall under the Indian Penal Code.

(i)	Sending threatening messages by email	Section 503 IPC
(ii)	Sending defamatory messages by email	Section 499 IPC
(iii)	Forgery of electronic records	Section 463 IPC
(iv)	Bogus websites, cyber frauds	Section 420 IPC
(v)	Email spoofing	Section 463 IPC
(vi)	Web-jacking	Section 383 IPC
(vii)	E-Mail Abuse	Section 500 IPC

 ISSN: 2582-6433

(viii)	Online sale of	Drugs	NDPS Act
(ix)	Online sale of	Arms	Arms Act
x)	Pornographic		Section 292 IPC

2.2 Cyber Crime and Criminal law of India:

Cyber crime is undefined concept, which means the criminal activity done by using the computer and internet. Cyber crime is a boundary less crime. Until the1999, Indian legal system has not concerned with any cyber law specially to control to the criminal activity. The present cyber law of India is creation of the e-commerce, because the concept of corporate world has undergone change and the multinational companies are working and require the protection in the new modes of the business. New modes of communication techniques are going to utilize by the businesscommunity. The internet makes available the easy and fast mode of communication tothe business world. The International community has also filled that for the globalization of the business it is necessary to introduce the new modes for the business. This globalization compels the international community to provide the regulation for the use of the internet. This leads to making of rules and regulation regarding the control of the e- business.

Though this internet and e-commerce emerged to make the easy and speedy communication, it impliedly provides the multiple opportunities to perform the illegal activities. When this illegal activity violates the right of someone as provided by anylaw, then it is the duty of the legal system to enact the lawsto protect from that act. Criminal law is the most important branch of the law, which closely connected with everyone. It is rightly says that criminal law is the best when it criminalizes least. Therefore, when the cyber crime ramped in the society, It need the effective criminallaw to curb it.

 ISSN: 2582-6433

The Information technology has invented the new world of cyber space. This world is the creation of the 21st Century. However, it is not like a physical world, however, it connected the world and makes it as a global village. Therefore, the work of legal system increased. Being a welfare state, it is duty of the state to protect the citizens in cyber space also. Therefore, it is necessary to the legal system to regulatethe activities in the cyber space. It is not subject of any particular country, but worldwide subject therefore the present cyber laws in the world are having transnational nature.

The Indian legal system has enacted Information Technology Act in the year 2000. The said act is mostly deals with the e-business and the regulation of e-commerce. Along with this, it recognized certain cyber crime. However, the Information Technology Act is enacted, Which deals with the regulation of digital signature and the authorities regarding it, The I.T. Act does not provide completely about the cyber crime but the other criminal law also deals withthe cyber crime. Indian Penal code also deals with the certain computer crime because cyber crime is new mode of the committing crime, which is not so much different from the conventional crime. However the cyber crime is committed by using the different modus operandi, therefore some amendments are require to cover the technical aspect. Therefore, the cyber law is enacted by the legal system. India is one of the countries among them, which are having alertness regarding the crimes going to be committedin cyber space.

2.2.1 Evolution of law in Cyber Space:

The modern world is of the cyber space, 21st century gives us a new world ofinternet. It drastically changes the life style of human being. Internet is now a lifeline in the present days. One or other way now connects everyone with computer. Every person generally using cell phone, laptop, tab computer etc. Computer takes place of paper and all records, so that personal data is now on computer or in the cyber space. So for protecting the personal information and data in the cyber space the laws are required. Cyber space represents the medium of communication, electronic. An internet or network of computers can operate without the constraints of space, state borders etc. Though they

 ISSN: 2582-6433

areonly a medium for storage, analysis and communication of information, communication that is fast outmoding or even replacing more traditional methodof communication. Therefore, cyber laws are the requirement and need of time.The convergence of the computer network and telecommunication facilitated by digital technologies has given birth to a common space called cyberspace.

The new shorter Oxford Dictionary explains the expression Cyberspace as, "the national environment within which electronic communication occurs, especially when represented as the inside of the computer system." [13]Space perceived as such by an observe but generated by a computer system and having no real existence, the space of virtual reality.

Traditional legal systems have had great difficulty in keeping peace with the rapid growth of the internet and its impact throughout the world. In spite ofthe recent fluency of legislation world-wide, it is unlikely that court and legislators will be able to provide sufficient guidance in a timely fashion to business to enable them to engagein commerce on or otherwise take advantage of the internet in a manner that avoids or minimize unexpected consequences or liabilities.

An internet or network of computers can operate without the constraints of space, state borders etc. Though they are only a medium for storage, analysis and communication of information, they virtually create a world of their own a medium inwhich a business can be transacted without any of the inhibitions that the real world imposes.

The main functions of the internet have thus emerged as providing

1. A cheap, fast relatively insecure means of international communication of text, sound and image,
2. A method of publishing information internationally,

 ISSN: 2582-6433

[13] https://en.oxforddictionaries.com/definition/cyberspace last access on dated APRIL 2023 at 5 .00 pm.

 ISSN: 2582-6433

Further challenges are presented by the need for security in electronic network. Government is in favors of the security but not for criminal or subversion communications. The growth in international crime has increased the need for the Government's ability to break corruption of unlawful communication, but lawful communication must be subject to the same link.

2.2.2 Indian Law on cyber crime

India also, like other countries of western has a well-developed legal infrastructure and it is going with the development and time. The result of this, Indiatoo is sharing the legal liability, which is the outcome of the technological boom. Though the India is having rich heritage of the legal system, then alsoit facing the problem of the traditional notion of the jurisdiction which is the great difficulty for thelaws related to the cyber space.

India has emerged as a world's leader in the field of Information technology , because the earning from the software and the IT services is nicely contributingthe Indian economy. With increasing in the growth and development of information technology and cyber world, the possibility of increase in the crime relating to computers has also increased simultaneously. Legislative steps for regulating the electronic commerce and checking the cyber crimes have also become essential. The Indian Parliament therefore enacted the Information Technology Act, 2000. For combating crime problem The Indian response in the form of legislative action as well as the IT revolution is mainly limited to this Act and Rules and Regulation made thereunder.[14]

[14] Laws on Cyber Crime: P.K.Singh (2007), Book Enclave, Jaipur, Page 23

 ISSN: 2582-6433

Committed where in any right is going to be violated, the conventional law provides the remedy. The offences as hacking is violation of right of privacyas recognized a fundamental Rights by the Apex Court of India. However, considering the need of International Society and for giving effect to the UN resolution the Indianlegal system require the law relating to the computer and Internet therefore the Information Technology Act and certain special rulesenacted by the Indian legal system. Due to certain technical nature, certain amendments also need therefore the Indian Legal system formulated the rulesto maintain its legal status in international family.

To meet the need of 21st Century the Indian legal system deals with the laws relating to the cyber space and cyber crime as following:

1. Information Technology Act:

To regulate the electronic communication the Indian Parliament has enacted thisAct, which involve the use of alternatives to the paper base means of communication and storage of information, to facilitate the electronic filing withthe government agencies. Along with the enactment of the IT Act 2000, to recognize theelectronic communication certain important amendments has made in the Indian laws, the amendments are required to make the execution of the regular laws in the information technology age. The main object of the IT Act is to facilitate legal reorganization and regulation of commercial activities through electronic medium. This Indian Act is based mainly on the United Nations resolution No A/GES/51/162; Dated 30th January, 1997, as well as on the UNICITRAL Model Law on Electronic Commerce.[15] This is only one act in Indian legal system, which known as the Cyber Law of India.

[15] IT Act 2000 vs 2008- Implementation, Challenges, and the role of adjudicating officers. By Karnikaseth

 ISSN: 2582-6433

and the recognition of the digital signature. As K.P. Singh has rightly pointedout themajor issue covered under the provision of the act are as following[16].

a) Establish rules which recognize and validate contracts and execution throughelectronic mediums;

b) Recognizes the admission of computer evidence in courts and arbitrationproceedings

The law is enacted to meet the digital technology and new communication technology and it also provides penalties for misuse or illegal use of technologyin certain situation therefore it is known as cyber law of India. As per the preamble of the Act, the object is more dealing with the electronic communication and the contract, which made through the internet. The preamble of Act says there is need forbringing in suitable amendments in the existing laws in our country to facilitate e- commerce.

Nature of the I.T. Act, 2000:

It is well recognized that it is mainly enacted to recognized and facilitate e- commerce and not to govern cyber crimes, however the Act defines certain offencesand penalties. Chapter XI of the act deals with offences and the ChapterIX deals with penalties and the authorities regarding adjudication. These two chapters of the I.T. actdeals with certain cyber crimes. Chapter IX focus on the following important features:

a) Regulating conduct in its unique way;

[16] Laws on Cyber Crime: P.K.Singh (2007), Book Enclave, Jaipur, First Publication. Page 96.

 ISSN: 2582-6433

b) Civil regulations to be employed by premise rather than criminal;

c) The process of adjudication is entrusted to adjudicating officersrather thanregular civil courts;

d) Such adjudicating officers are required to know the laws and theIT or musthave judicial experience;

e) Adjudicating officers are vested with power of civil court;

f) The proceeding to be conducted by such adjudicating officers areto be construed as judicial proceedings;

g) The quantum of compensation to be calculated at market rate forloss or sufferings.

This features shows that this chapter mere gives of civil court, certain provisions deals with power to impose the penalty. When these provisions of IT Actwhich deals with the civil liability, and if the act is comes under any penal provisionof Criminal law, then it can registered under that Laws also.

Chapter XI of the Act defines certain offences and prescribed the punishmentfor that cyber crimes. For example, Section 65 of the Act deals with the offenceof Tampering with the computer source document. The wording of the tampering is as following:

Section 65: Tampering with Computer Source Document: Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer sources code use for a computer with fine which may be extendedup to two lakh rupees or both .[17]

This is the penal section of the IT Act, which deals with concealing or distorting the source of the computer. This offence deals with the privacy

[17] Section 65, The Indian Information Technology Act , 2000

 ISSN: 2582-6433

of the computers accession. For this, the punishment is provided up to the three years. Thissection essentially tries to stop the efforts or actions or commands givento the computer to alter the programs, destroy the programs or to cancel them in such a waythat they cannot be used by the person who owns the program. Whether this is intentional or mischievous act but it attracts the punishment upto three years or fine up to two lakhs rupees.

This section enacted mainly to protect the institution where the important data isgoing to be kept or stored. The most important step, which an organization shouldtake is to register its source Code. There are times when it becomes difficult for an organization to prove that a particular source code was there property as one of the ex-employees might take away the code to see in other company. There, if the organization has registered its source code then it is easyto pin down the culprit.[51]

Like this there are further section 66, 67, 70 etc. which deals with the offences as like hacking the computer or offence of obscene publication in electronic form.Section 65 to 75 of the IT Act deals especially with the cyber crimes and the punishments for that, but these are not the all forms of the cyber crime. All these offences deals with the criminal act though it is similar to the conventional crime, where in the computer is either tool or target while committing that crime.

Section 66 deals with the offence of unauthorized access to the computerresource. In the language of the computer, it is called hacking. The act in this offenceis going to be committed by using the dishonest intention. [18]

[18] Cyber Law & Crime : Barkha U Rama Mohan (2011) Asia Law House, Hyderabad. Page 1.

 ISSN: 2582-6433

1. Information Technology (Certifying Authorities) Rules, 2000

2. Information Technology (Security Procedure) Rules, 2004

3. Information Technology (Certifying Authority) Regulations, 2001

As the said act also cannot fulfill the need of the time and the cyber security is facing the problem as well as the execution is impossible due to certain technical problem. Therefore, the Information Technology Act is drastically amended in the year 2008. The said amendment has made to bring the cyber crime under the preview of the conventional law.

The Information Technology (Amendment) Act, 2008

After the execution from the 2000, the IT Act is facing difficulties while executing. Due to certain technical loopholes in I T Act, 2000, the amendment is sought to for the smooth execution of the Act; the amendment takes placein 2008, which has changed the nature of the I.T. Act. To meet the hurdles forthe enforcement certain important sections are inserted in the I T Act and it brought the various illegalactivities on computer in the preview of cyber crime in this Act The Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought remarkable changes in the IT Act, 2000 on several counts.

The amendment added certain important definitions in the Act, Section 2(ha) is added "Communication device" which bring the cell phone under the previewof cyber crime. This amendment brings all communication devices, cell phones, iPods or other devices used to communicate, send or transmit any text, video, audio or image. Section 2 (w) has also bring the service providers under the preview of cyber crime. The amendment Act also inserted various new things in the Act as like the controlling authority, power of adjudicative authority. However, more important is that, certain provisions regarding the offences are included in the Act.

 ISSN: 2582-6433

New cybercrime under I T Amendment Act, 2008:

Many cybercrimes for which no express provisions existed in the IT Act, 2000 now included by the IT (Amendment) Act, 2008. This Act adds new provisionsin section 66,as like Sending of offensive or false messages (s 66A), receiving stolen computer resource (s 66B), identity theft (s 66C), cheating by personation (s 66D),

Violation of privacy (s 66E). These all things though concern with the privacy rights but that is going to violated by different mode so it require to be in the Act. A new offence of Cyber terrorism is added in Section 66 F which prescribes punishment thatmay extend to imprisonment for life. Section 66 F, covers any act committed with intent to threaten unity, integrity, security or sovereignty of India or cause terror by causing DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty or integrity of India, the security, friendly relations with other states, public order, decency, morality, or in relation to contempt of court, defamation or incitement to an offence, or to advantage of any foreign nation, group of individuals or otherwise. These offences are more important because the offencesagainst the nation are now going to be committed by using new techniques of the communication.

For other offences mentioned in Section 66, punishment prescribed is generally up to three years and fine of one/two lakhs has been prescribed and these offences are cognizable and bailable. This will not prove to play a deterrent factor forcyber criminals. Further, as per new Section 84B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and thenew Section 84C makes attempt to commit an offence also a punishable offence withimprisonment for a term, which may extend to one- half of the longest term of imprisonment provided for that offence.

In certain offences, such as hacking (sec 66) punishment is enhanced from three years of imprisonment and fine of two lakhs to fine of five lakhs. In Section 67, for publishing of obscene information imprisonment term has been reduced from fiveyears

 ISSN: 2582-6433

to three years (and five years for subsequent offence instead of earlier ten years) and fine has been increased from one lakh to five lakhs (rupees ten lakhs onsubsequent conviction). Section 67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that may extend to five years with fine up to ten lakhs. This provision was essential to curb MMS attacks and video voyeurism. Section 67B punishes offence of child pornography, child's sexually explicit actor conduct with imprisonment on first conviction for a term up to five years and fine up to ten lakhs. This is a positive change as it makes even browsing and collecting of child pornography a punishable offence.

Punishment for disclosure of information in breach of lawful contract under Section 72 is increased from two yrs up to five yrs and from one lakh to five lakhs or both. This will deter the commission of such crime. By virtue of Section 84 B personwho abets a cybercrime will be punished with punishment provided for that offence under the Act. This provision will play a deterrent role and prevent commission of conspiracy linked cybercrimes. In addition, punishment for attempt to commit offences is given under Section 84 C, which will be punishable with one half of the term of imprisonment prescribed for that offence or such fine as provided or both.

Thus, the important changes takes place in I.T. Act 2008, which brings the various crimes, which are committed by using the computer or any communication device. Then also various cyber crimes are going to be registered using the Indian Penal Code. It shows that the Amendment cannot cover all the cyber crimes, becausethe cyber crime is basically different from the conventional crime, however the way to commit the crime is changed and the computer is a tool to commit the crime or in certain crime it is target.[19]

2. Indian Penal Code .1860

Indian Penal code is the universal criminal law of India. The base to constitute the offence is nothing but the guilty intention and prohibited act according to the Indian Penal code. The Indian penal code is basic criminal law of India, along with the time, the legal system enacted certain special criminal law. The cyber crime is creation of information technology age, though the modes or ways to commits cybercrime is

 ISSN: 2582-6433

different from the conventional crime, but it is not much different from the conventional crime. The IT Act has not covered all the cyber crimes; again, Indian Penal code is applicable. Due to the universal nature of the IPC, it covers almost all the crime.

Therefore the enactment of Information technology compel the law makers to amend the Indian Penal code, which is called as a conventional Penal law of India. The First schedule to the Information Technology Act of 2000 has amended the certain provisions of Indian Penal code, 1860. The amended provision have been widened to include offences involving electronic record.

Sec. 192 of the Indian Penal code has amended the meaning of fabricating false evidence to include any false entry or electronic records containing a false statement. The word electronic record is creation of this digital world. When the electronic record is comes under the preview of the Indian Penal code, thenmost of the offences relating the documents which are committed by way of computer are comes under the jurisdiction of Indian penal code, though they are known as a cyber crimes. Section 192 deals with the fabricating falseevidence, whenever any electronic record is falsely made which provided for the judicial proceeding then it amount to be fabricating false evidence.

[19] http://catindia.gov.in/writereaddata/ev_rvnrbv111912012.pdf last access on dated APRIL 2023at9.21pm.

 ISSN: 2582-6433

This offence can be committed by using the computer as a tool, and then also it is subject to the Indian Penal code, apart from this the crime like web- jacking, threatening emails etc. are within the preview of section 383 of Indian Penal code dealing with the extortion. Whoever intentionally puts any person in fear of injury tothat person, or to any other and thereby dishonestly induce the person so put in fear to deliver any property or valuable security or anything signed or sealed, which may be converted into a valuable security, commits extortion. This offence can also be committed by sending threading emails, Information technology Act provide the punishment for this crime but it can be penalized under Indian Penal Code.

Fraud on the internet is big business. Most of the cyber crimes comes in the category of fraud, but the Information Technology Act has not define the concept of fraud therefore most of the offences comes under the preview of the Indian Penal Code. Section 25 of IPC definitions fraudulently as a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise. The IT Act Section 66B used the word "dishonest intention" which is not defined in the IT Act then one can refer to IPC, which is a general legislation in the area of criminal law.

When any cyber fraud is committed in real sense it would be cheating which is defined in section 415 of I.P.C. when any person makes the cheating by using internet it is very easy to him to hide his identity, this act perfectly comes it the offence provided under section 416 of I.P.C. that is cheating by personation. Apart from thisvarious cyber offences are relevant under the sections as like 405,406,463,465 of I.P.C. even the launching of virus is provided under section 43 of I.T.ACT is comesunder the preview of sec. 425 of I.P.C. The act of launching of virus and other computer contaminants, would also amount to criminal offence of mischief. If the essentials of mischief are satisfied it would be an offence too.

Thus, the Indian Penal Code almost covers various cyber crimes, but considering the needs and development along with the information Technology Act certain important amendments made in Indian Penal Code in 2000. The amendmentsaresought to bring the

 ISSN: 2582-6433

paperless transactions under the preview of conventional criminal law. This amendment is suitable in the age of electronic commerce. Due to amendment the Act eliminated the basic requirement of paperless record and documents because substantive as well as procedural law, Indian Penal code, 1860, Indian Evidence Act, 1872 and even Criminal Procedure Code.

In Indian Penal Code the certain words as like 'computer resources' or 'electronic record' are inserted in various sections as like section 119,167,173,175etc. Thus, the Indian Penal Code covers the cyber crime. Even the Criminal Law Amendment Act 2013 has inserted certain sections, which are covering the offences which are going to be committed by using the computer or any communication device. Section 354 C deals with voyeurism and Section 354 stalking, these offencesare subjected to the internet and communication device. Therefore the cyber crime though new kind of offences are subjected to the Indian Penal code. If we see the Section 354D. it is as following

Sec. 354D. Stalking – (1) Any man who-

(i) Follows a woman and contacts, or attempts to contact such womanto foster personal interaction repeatedly despite a clear indication of disinterest by suchwoman; or

(ii) Monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.

Provided that such conduct shall not amount to stalking if the man who pursuedit proves that-

(i) It was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

(ii) It was pursued under any law or to comply with any condition or requirementimposed by any person under any law; or

(iii) In the particular circumstances such conduct was reasonable and justified.

 ISSN: 2582-6433

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extendto three years, and shall also be liable to fine; and be punished on a second or subsequentconviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

Thus, the Indian penal code covers the cyber crime. There are various well known cyber crimes, which are not contended in Information Technology Act, But that covers in the Indian Peal Code.

Cyber crimes in Indian Penal Code

(a) Cyber Stalking

There is no universally accepted definition of cyber Stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using Internet services. Stalking in General terms canbe referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victimsproperty, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It alldepends on the course of conduct of the stalker. It is made punishable under section 354D of IPC.

(b) Cyber squatting

Cyber squatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different). A trademark owner can prevail in a cyber squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domainname in connection with thesale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of-pocket

 ISSN: 2582-6433

expenses.

(c) Data Diddling

This kind of attack involves altering the raw data just before a computerprocesses it and then changing it back after the processing is completed.

(d) Cyber Defamation

Cyber defamation is not too much different than the defamation provided in Sec.499 of IPC .it is nothing but any derogatory statement, which designed to injure aperson's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers or the Internet, as like, someone publishes defamatory matter about someone on a website or sends e- mails containing defamatory information to all of that person's friends.

(e) Trojan Attack

A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing whatit is actually doing.

(f) Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. It is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in college.

(g) Financial crimes

This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC and IT Act. Therefore when suck crimestakesplace, both laws can be attracted. A leading Bank in India was cheated tothe extent of 1.39 corers due to misappropriation of funds by manipulation of computer recordsregarding debit and

 ISSN: 2582-6433

credit accounts.

(h) Internet time theft

It is nothing but one kind of cheating, where the internet is tool for committing this crime. This can notes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cyber crime was unheard until the victim reported it. This offence is usually covered under IPC and the Indian Telegraph Act.

(i) Virus/worm attack

Virus is a program that attaches it selves to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or by deleting it. Worms, unlike viruses do not need the host to attach themselves They merely make functional copies of themselvesand do this repeatedly until they eat up all the available space on a computer's memory. This is one kind of trespass in the conventional crime. Though it is purely acyber crime, It covers under the Indian Penal code.

(j) E-mail spoofing

It is a kind of e-mail that appears to originate from one source although it hasactually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B's friend containing ill about him by spoofing B's email address, this could result in ending of relations between B and his friends.

(k) Email bombing

Email bombing means sending large amount of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can varyfrom individuals to companies and even the email service provider. This isone kind of the mischief, where in the account or server is subject to destructs.

(l) Salami attack

This is basically related to finance and therefore the main victims of this crimearethe financial institutions. This attack has a unique quality that the alteration is so

 ISSN: 2582-6433

insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program whereby a meager sum of Rs 3 is deducted from customers account. Such a small amount will not be noticeable at all.

However, due

such merger from all the account holders collect huge amount. This is purely acriminal breach of contract.

(m) Web Jacking

This term has taken from the word hijacking. Once a website is web jacked the owner of the site looses all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site. As it isone kind of hacking, but the IT Act has not use the word hacking specially, but dealswith the various kind of unauthorized access or tampering with the computer resources, IT Act cannot cover all kind of hacking therefore IPC is generally applicable to such kind of the unauthorized access.

These are the offences, which are subject to the Indian Penal code and without the general principles of criminal law and specially Indian Penal Code; cyber law cannot work in India. However, the nature of offences changes, the base ofthe crime is quite same. Therefore, IPC is having wider scope even in conventional crime and the cyber crime in India

3. Indian Evidence Act and Criminal procedure Code

These are two important procedural laws in Indian legal system. Both aredealing with the procedure of criminal proceeding. Due to increasing crimes of fraudthrough the computer and internet, these Act are also required to amend and make suitable for the information technology age. Considering the need equired changes have been made in the Indian Evidence Act, Indian Penal Code and Criminal Procedure Code by the Indian Parliament on December 23, 2008 with the passing of Amended IT Bill 2006. In Indian Evidence Act, Section 3 relating to interpretation clause words 'Digital Signature' and 'Digital Signature Certificate', the words 'Electronic Signature' and 'Electronic Signature Certificate' are substituted.

 ISSN: 2582-6433

In Criminal Procedure Code, after Section 198 A[20], Section 198 B has been inserted according to which, "No Court shall take cognizance of an offence punishable under Sections 417, 419 and 502 of the Indian Penal Code, except upon acomplaint made by the person aggrieved by the offence". Moreover in the Indian Penal Code the meaning of some words like "offences" and "computer resource" has

been made more exhaustive which take colour from the IT Act, 2000. It showsthat India is successful in facing new challenges of IT. Many amendments have been made in the Copy Right Act on the argument that certain knowledge should be treated as private property and capable of 'Ownership'. Considering the requirement of society now, cyber law is providing a worth in administration of justice.

4. Cyber laws in India.

[20] Section 198 A of Cr. P.C. 1973

 ISSN: 2582-6433

Apart from the Information Technology Act and Indian Penal Code, there are certain laws and regulations, which deal with the cyber crime. Even certain civil lawsare relevant in certain misuse in cyber space. However, generally the fraud is there incyber crime, therefore it concerns with the criminal law, otherwise even Law of Tort is also relevant and can provide the remedy to unauthorized use of the computer andinternet. Apart from The Information Technology Act 2000 and Indian Penal Code 1860, there are various other laws relating to cyber crime in India. They are as following.

1. Common Law (governed by general principles of law)
2. The Bankers' Book Evidence Act, 1891
3. The Reserve Bank of India Act, 1934
4. The Information Technology (Amendment) Act, 2008 and 2009
5. The Information Technology (Removal of difficulties) Order, 2002
6. The Information Technology (Certifying Authorities) Rules, 2000
7. The Information Technology (Certifying Authorities) Regulations, 2001
8. The Information Technology (Securities Procedure) Rules, 2004
9. Various laws relating to IPRs.

Thus, the Indian legal system is having various laws concerning the cyber crimes. But the nature of the cyber crime is technical, therefore it require the technical process to execute the criminal law in proper sense. The technical process is lacking in Indian legal system, therefore though the substantive criminal law is sufficient, but due to lacking in procedural aspect its unable to execute it in India. The basic problemin the cyber crime is that, there is specific manner by which the internet can be misuse; it is on the criminals, that they always misuse it in different manner, therefore it is not possible to the legal system to meet with the need. Apart from this, the nature of cyber crime is transnational, therefore it required the international co-operation. Mere making laws is not sufficient, cyber law cannot work without the international co-operation. The Information Technology Act 2000 and all the related laws having provision regarding the transnationaljurisdiction, but execution is possible when all countries in the world recognized that act as a crime, and allow the proceeding on

 ISSN: 2582-6433

thataspect.