



INTERNATIONAL LAW  
JOURNAL

---

**WHITE BLACK  
LEGAL LAW  
JOURNAL  
ISSN: 2581-  
8503**

**Peer - Reviewed & Refereed Journal**

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

[WWW.WHITEBLACKLEGAL.CO.IN](http://WWW.WHITEBLACKLEGAL.CO.IN)

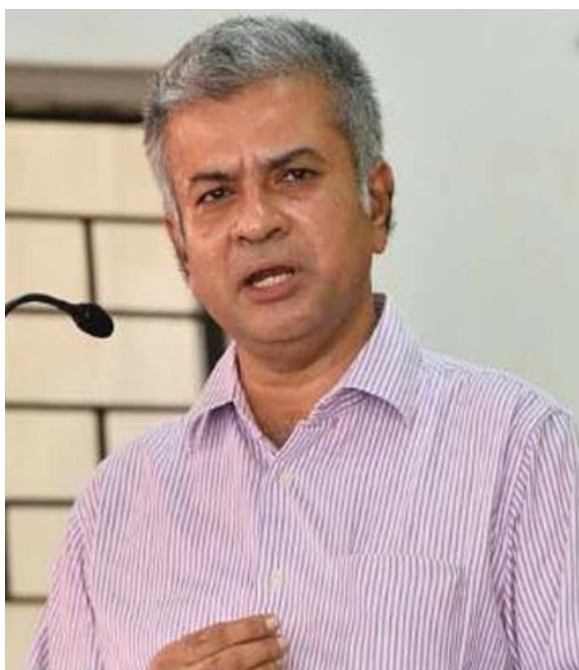
## **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK  
LEGAL

## **EDITORIAL TEAM**

### **Raju Narayana Swamy (IAS ) Indian Administrative Service officer**



a professional  
Procurement from the World Bank.

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) ( with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public

### **Dr. R. K. Upadhyay**

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



## **Senior Editor**

### **Dr. Neha Mishra**



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

### **Ms. Sumiti Ahuja**

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.





### **Dr. Navtika Singh Nautiyal**

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



### **Dr. Rinu Saraswat**

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

### **Dr. Nitesh Saraswat**

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

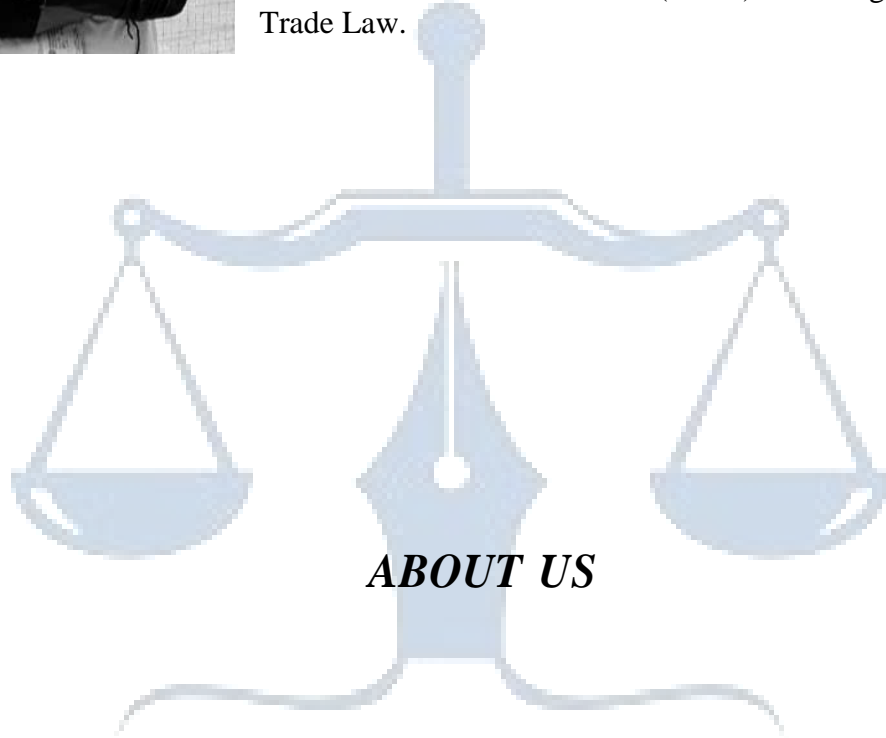




## **Subhrajit Chanda**

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.



## ***ABOUT US***

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provided dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you



WHITE BLACK  
LEGAL

# LAWS FOR COMBATING CYBER CRIMES IN INDIA: A CRITICAL STUDY.

AUTHORED BY – DHRUV BHATI

## LIST OF CASES

1. Ranjit D. Udeshi v. State of Maharashtra AIR 1965 SC 881.
2. Samaresh Bose v. Amal Mitra (1985) 4 SCC 289.
3. Miller v. California 413 US 15 (1973).
4. Director General, Directorate General of Doordarshan v. Anand Patwardhan & Anr 1996 (8) SCC 433.
5. Ajay Goswami v. Union of India AIR 2007 SC 493.
6. Maqbool Fida Hussain v. Raj Kumar Pandey Crl. Revision Petition No.114/2007.
7. State of Tamil Nadu v. Suhas Katti, 2004.
8. State of Tamil Nadu v. Dr. L. Prakash 2002 Cri L J 2596.
9. Wilhelmus Weijdeveld v. India, 2009./article/20110527/ARTICLE/305279912/1028.
10. Avinash Bajaj v. State (NCT) of Delhi (2005) 3 CompLj 364 Del, 116(2005) DLT427, 2005 (79) DRJ 576.
11. Ritu Kohli Case.
12. Manubhai Shah v. Life Insurance Corp. of India, [1992] 3 SCC 637.



13. Shreya Singhal v. Union of India MANU/SC/0329/2015.
14. Sakal Papers (P) Ltd. & Ors. v. Union of India, [1962] 3 S.C.R. 842.
15. Romesh Thappar v. The State of Madras, 1950 AIR 124,1950 SCR 594.
16. Bennett Coleman & Co. & Ors. v. Union of India & Ors., [1973] 2 S.C.R.757 at 829.
17. S. Khushboo v. Kanniamal & Anr., (2010) 5, SCC 600.
18. Vinod Kaushik & another v. Nidhi Joshi. Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez Case.
19. Ambikesh Mahapatra & another v. State of West Bengal & others, [2015] SCC CAL631(71).
20. Anvar P.V. v. P.K. Basheer MANU/SC/0834/2014.
21. Dharambir v. Central Bureau of Investigation MANU/DE/0392/2008.
22. Rishi Narula Vs. The State Nct of Delhi and Ors. MANU/DE/5313/2016.
23. Sharat Babu Digumarti v. State, Govt. of NCT of Delhi MANU/DE/2615/2015.
24. K.A. Abbas v. Union of India and Anr AIR 1971 SC 481.
25. Chandrakant Kayandas Kakodar vs The State of Maharashtra 1970 AIR 1390
26. Aveek Sarkar v. State of West Bengal (2014) 4 SCC 257.
27. Bobby Art International & Ors. v. Ompal Singh Hoon (1996) SC 1846,



WHITE BLACK  
LEGAL

## ABBREVIATIONS

AIR : All India Reports

ASP : Access Service Provider

BBEA : Banker's Books Evidence Act

BSNL : Bharat Sanchar Nigam Limited

CDA: Communication Decency Act, US

CrPC : Criminal Procedure Code, 1972

CCC: Cyber Crime Cell

CBI : Central Bureau of Investigation

CCRC : Computer Crime Research Centre

CERT : Computer Emergency Response Team

CFAA : Computer Fraud and Abuse Act

CrLJ: Criminal Law Journal

CMA : Computer Misuse Act

DCT: Digital Communication Technology

DMCA: Digital Millennium Copy Right Act, us

DPA : Data Protection Act

EU : European Union

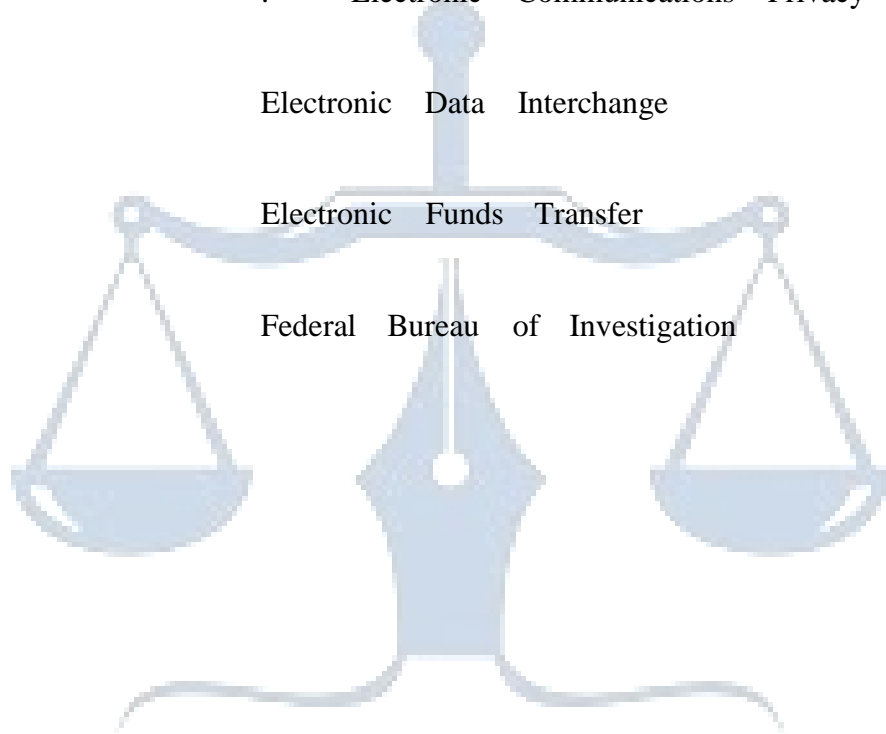
EA : Electronic Attack

ECPA : Electronic Communications Privacy Act

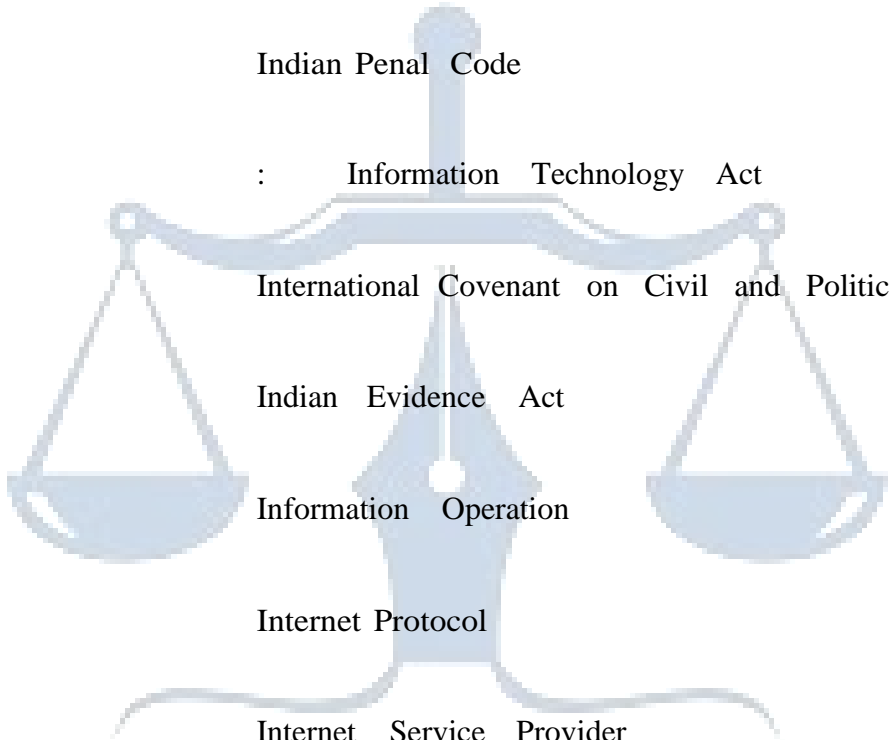
EDI : Electronic Data Interchange

EFT : Electronic Funds Transfer

FBI : Federal Bureau of Investigation



WHITE BLACK  
LEGAL



FTP : File Transfer Protocol

HC : High Court

HTML: Hypertext Markup Language

ICT : Internet Communication Technology

IPC : Indian Penal Code

IT Act : Information Technology Act

ICCPR: International Covenant on Civil and Political

IEA : Indian Evidence Act

IO : Information Operation

IP : Internet Protocol

ISP : Internet Service Provider

LGBT : Lesbian, Gay, Bisexual, Transgender

LAN: Local Area Network

LR : Law Reporter

MMS : Multimedia Messaging Service

MPSNS : Multipurpose Social Networking Sites

MNOs : Mobile Network Operators

No. : Number

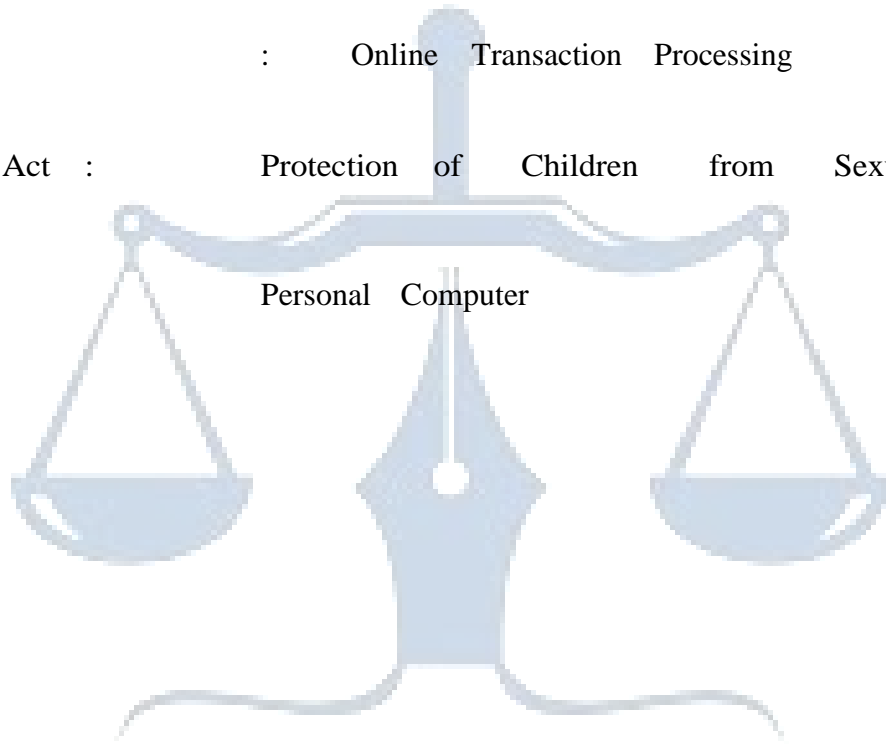
NIPC : National Infrastructure Protection Centre

NEFT : National Electronics Funds Transfer

OLPT : Online Transaction Processing

POCSO Act : Protection of Children from Sexual Act,  
2012

PC : Personal Computer



WHITE BLACK  
LEGAL

PICS: Platform for Internet Content Selection

PKI : Public Key Infrastructure

PNC : Police National Computer

RBI : Reserve Bank of India

RIPA : Registration of Investigatory Powers Act

RTGS : Real Time Gross Settlement

SC : Supreme Court

SCC : Supreme court Cases

Sch : Schedule

SIM : Subscriber Identity Module

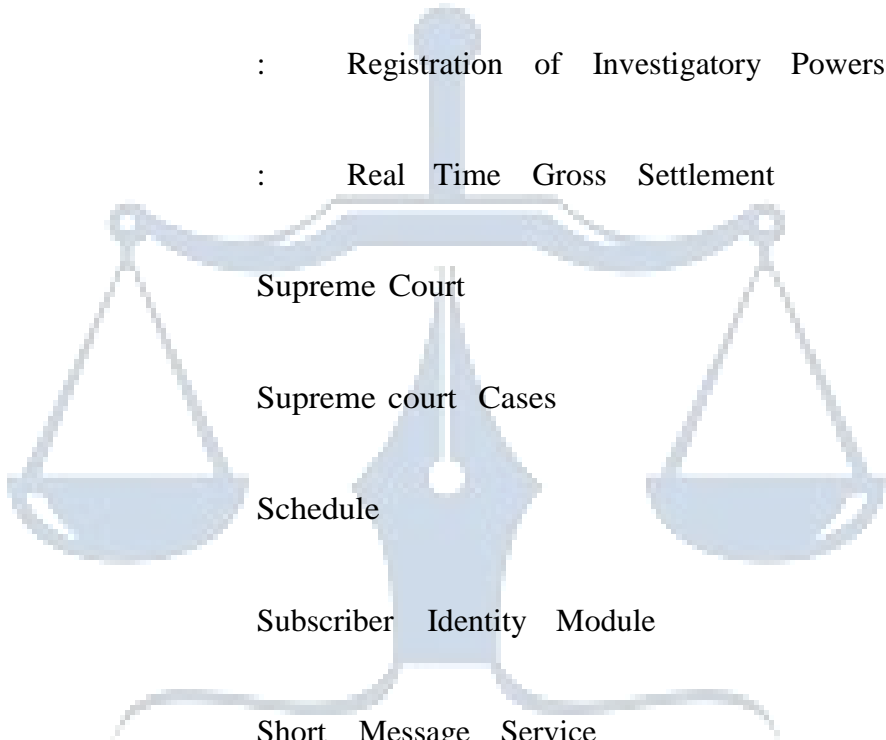
SMS : Short Message Service

SNWS : Social Networking Sites

SET : Secure Electronic Transfer

TELNET : Telecommunication Network

TRAI : Telecom Regulatory Authority of India



WHITE BLACK  
LEGAL

## 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 being is 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 every developed 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 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 on the social structure of the society. Especially the Indian culture is quite different but the information technology has connected the people. The social sites makes the platform



to the nonprofessional to share their view, but along with the good impacts 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. As per 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. *“Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either 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 means for perpetuating further crimes comes within the ambit of cyber crime”*.

Cyber crime is an evil having its origin in the growing dependence on computers in 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 for committing the crime or an illegal act by using the means of computer.

The internet is a technical development gives us all opportunity to act as global community. Internet and electronic based trading affect all aspects of business. The information technology revolution is creating new business and forgoing old one to either change or die. The traditional legal systems have a great difficulty in keeping pace 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 and related offences, which are nothing, but relating to the offences outraging the modesty of 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 has been changed so it requires different tools for investigation. The basic intention behind 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 and criminal misappropriation or fraud. Therefore, the cyber crime is not different from the conventional crime and subject to the regular criminal law of India.

The present era is welfare state, its first and foremost duty is to maintain peace and security. Effective criminal law is required to maintain peace and security. So far as the Indian legal system

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 Penal code cover all the crimes as contended the conventional crime, and for the execution of this law, effective investigation is required, and therefore the Criminal procedure code<sup>1</sup> deals with the investigation and powers to investigate. Execution of criminal law is 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. For this, the 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 21<sup>st</sup> century, but the object of the cyber criminals, is nothing but wrongful gain or wrongful loss, or in certain cases with intention to devalue 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

---

<sup>1</sup> Guide to cyber Laws, Rodney D. Ryder,(2003) Wadhwa Nagpur, Page 2.



WHITE BLACK  
LEGAL

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 21<sup>st</sup> century, but the object of the cyber criminals, is nothing but wrongful gain or wrongful loss, or in certain cases with intention 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 has also developed with the changing of the time. The law is subject to the 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 is going to be committed by using the technology, such as the Indian Penal Code sec 354(D) which deals with the Stalking.

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. Due to this aspect whether the present criminal law of India including the procedural and substantive 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 present laws and it utility to control the 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 provisions which cover the offences like cyber crimes.
- 2.To make the study of cyber law including I T Act and the relevant Penal provisions pertaining to cyber crime.
- 3.To make the comparative study of conventional Criminal law of Indian and cyber crime and laws relating to cyber crime

To find out the shortcoming of the laws pertaining to cyber crime including the procedural laws i.e. The Code of Criminal Procedure and Indian 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 developed stage 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 laws also 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 are subject 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 it also 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 always changes 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 developed in present days. Internet is the essential part of the human beings life today. Internet make the world a globe, which bring 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 cyber crime 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 provisions of 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 Indian legal 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 of the said section. While reading the section from the book, we can easily understand the nature of the sections object 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



WHITE BLACK  
LEGAL

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 basic principles behind the section, in simple the base of that section. The author discussed the 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 Era Law Publication, Delhi (2004)**

This book is best research in the era of the cyber law. This is the research on the problem of the jurisdiction in cyber crime. The peculiar character of cyber crime is that, 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. In conventional crime and criminal law, the land laws regulate the crime and having power to control and curbit. However, in cyber crime the problem of jurisdictions arises. This book help to understand the problem of jurisdiction in cyber crime and the solution which international community has tries to provide is discussed by the author.

The author discuss the cyber law from all angle, its inanition, howbusiness law turn 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 day a 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 cyber space 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 thisinternet transaction, the first International convention on the online transaction has discussed by the author. The author discussed theInternational 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 ofit along with the commentary. The book is useful to the researchers.

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

Hyd.3rd edition.2011



WHITE BLACK  
LEGAL

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 help the research to deals with the practical problem in the cyber crime investigation and the difficulty in the 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 discusses how the misuse of technology affects the right of individual as like the right of privacy. Now interfering in the privacy of person by using the technology of computer is amount to the 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 cybercrime. Cyber crime investigation is now a complex issue before the investigation machinery due 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



WHITE BLACK  
LEGAL

**Delhi 8th edi 2004.**

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 the said crimes. The Information technology Act is quite business law and the offences 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 on the 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 Technology Act 2000 and the related issue.

WHITE BLACK  
LEGAL

**Hypothesis:**

Indian Criminal law is now well developed; so for an 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



WHITE BLACK  
LEGAL



cyber crime. In 1978 the concept of internet was emerge and in 1989, the foundation 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. Cyber crime 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 has not amended in such a way that is why the problem of cyber crime is increase and need 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 new policies 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 appointed 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 inlaw and computer.



WHITE BLACK  
LEGAL

## **Research Methodology:**

Considering the aims and objectives of the research the methodology is adopted literature review and research through accessing hard copy and electronic 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 the laws regarding cyber crime and conventional crime in India and Its amendment is the main 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 courts view 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 provides the results in all means for the research subject.



WHITE BLACK  
LEGAL

## 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 time immemorial. 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 20<sup>th</sup> 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 is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China.<sup>2</sup> Indian legal system 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 law is broader than the command. This role of law is more relevant in the present situation. The criminal law closely connected with the each member of the society. In the age of information technology, cyber law is need of hours. The cyber law means the law relating to the cyber crime.

WHITE BLACK  
LEGAL

---

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



WHITE BLACK  
LEGAL

A person sitting 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 entire world. 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, which deals 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 makes impact 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 internet can 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<sup>3</sup>.

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 and back by sanction. Now crime means a legal wrong. Initially it is somewhere the religious wrong when the religious institutions were powerful. There were no difference between sin and crime. However, along with the development of State, the concept of sin was diluted and the sin or wrongful act term in to a wrongful act. This wrongful act now turns in to the concept of crime or offence. According to Granville Williams, crime or offence is 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 commit the crime, it is called a cyber crime. Cyber crime is not new but it is as like the conventional crime. Basically the 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 crime can be called as a cyber crime. When the word cyber comes, it deals always with the computer or any network. When this computer or internet is used to commit a

---

<sup>3</sup> Cyber crime- Law & policy perspectives, Dr. Mrs. K. Sita Manikyam (APRIL 23)



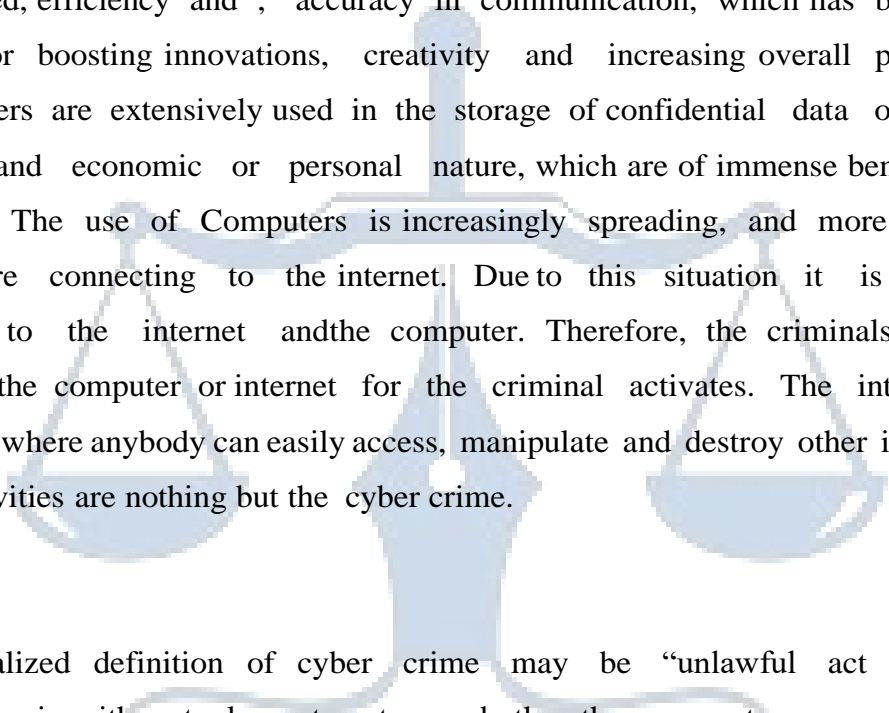
WHITE BLACK  
LEGAL



crime, it is cyber crime. In cyber crime computer is an instrument to commit the crime or it may be a target.



WHITE BLACK  
LEGAL



In the present era of rapid growth, information technology is encompassing all lifestyles all over the world. These technological developments made the transition for paper to paperless transaction possible. We are now creating new standards of speed, efficiency and , accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used 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 activities. 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; this kind 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. The sine qua 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 as cyber crime. This information



WHITE BLACK  
LEGAL

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 the wonder 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, the computer world may exist only in intangible form, it affects the physical and real environment. 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, though it is not possible to define the cyber crime, but it is 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 any crime 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 a wide 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 illegal act requiring knowledge of computer Technology for its perpetration, investigation or prosecution". However, the definition is not exhaustive as there are many acts, which can 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.<sup>4</sup>

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 automatic processing 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

---

<sup>4</sup> Cybercrime: Talat Fatima, (2011) Eastern Book Company, Lucknow. Page 89.



WHITE BLACK  
LEGAL

illegal activities pertaining to the data transmission. However, the cyber crime not only deals with the data 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) content-related offence; 4) offences related to infringements of copyright and related rights.<sup>5</sup>

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 cover all the activities in which the privacy of some once going too violated by using 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 definition is very broader in sense cannot give any precise meaning of 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 complete concept of cyber crime. The countries have to enact the multiple laws to cover the misuse of the computer and related 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”

---

<sup>5</sup> Cyber Crime and National Security: The Role of The Penal and Procedural Law by  
Laura Ani



WHITE BLACK  
LEGAL



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 cyber crime that it ever requires the physical force. Whenever the person misuses the cyber space to 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 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 shallbe punishable with a fine which may extent up to rupees two lakhs or with imprisonment up to three years, or with both.”<sup>6</sup>

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; in other 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 made or could have made 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 access to 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

---

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



WHITE BLACK  
LEGAL

crime.

On these spelt, it shows the concept of the cyber crime. However, any authority 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 the cyber 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:**

The term cyber crime cannot define due to the critical nature of it, because it involves the crime relating to computer and computer techniques.<sup>36</sup> Therefore, it has not any specific ingredients different from conventional crime apart from the techniques. Because development of technology create new way to commit the crime called 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 crimes are 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 knowledge and skill can easily destroy valuable database causing huge loss or damage to the affected victims of the crime.<sup>7</sup>

Many a times even the victim affected by cyber crime is unaware of its occurrence because of lack of adequate skill and know how in handling the computer system.

---

<sup>7</sup> [tecindia.co.in/navneet/navneet-cyberlaw/MIR-012-B2](http://tecindia.co.in/navneet/navneet-cyberlaw/MIR-012-B2) last accesson



WHITE BLACK  
LEGAL

with the routine working system and has a good understanding of the loopholes and availability of opportunities to commit the cyber crime without leaving any trace for possible detection. Apart from the employees who are unhappy with their employees for one reason or the other may tend to target the employees computer system to take revenge 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.<sup>8</sup>

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-economic and the legal rights of the people. Through, the use of computer network system in itself is legal but the illegal actions in using the networks as a medium are deemed illegal and punishable under the criminal law or the cyber law or both. Like any other cyber crime 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 away from 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 20<sup>th</sup> century. It has drastically changed the

---

<sup>8</sup> U.N. Congress on prevention of crime & treatment of offenders held in viagna on April 2023

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. The computer and this internet bring cyber crime with it. Thus, cyber crime are unknown to the legal world prior to the birth to the internet and includes not only acts which are employed 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, therefore it 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. 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 the major cyber laws of the US and UK do not content a definition of cyber crime. However, the taxonomy of these 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 by the 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 criminologist gives different reason. Cyber crime is creation of the technology and the technology makes the 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. As Prof. H. L .A. Hart in his classic work entitled, "The concept of law"<sup>9</sup> 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 computer systems despite being hi-tech devices are extremely vulnerable Computeris 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 Moreand 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,

---

<sup>9</sup> Cyber Crimes: Law & Policy Perspectives, Dr.Mrs.K.Sita Manikyam , (2009)Hind Law House, Pune Page 41.



WHITE BLACK  
LEGAL



down loads etc. However, wider access to information creates some problems like protecting and guarding any computer system against unauthorized use.



WHITE BLACK  
LEGAL

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 room 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 turn are composed of millions of codes. Human mind is fallible and it is possible that there might 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 and security devices. Thus, hackers are the dreaded enemy of the internet and general network security and they exploit the complexity of computer systems motivated by personal vengeance. Sabotage fraud, greed 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



WHITE BLACK  
LEGAL

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 disseminating information or records has now been replaced by the digital computer processing and network technology. The real issue before law enforcement and investigating agencies is how to procure and preserve evidence unlike traditional offences, it is very difficult to 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 necessitated 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 to mislead the investigating agencies.

5) Jurisdictional Uncertainty<sup>10</sup>

---

<sup>10</sup> Conventional crime through computer e-book.

Cyber crimes cut across territorial borders which undermine the feasibility and legitimacy of applying domestic laws which are normally based on geographical 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 among the 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 not so 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 procedure governing cyber crimes the law enforcing authorities of individual countries find it 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 continue their 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 legal system. Therefore, it is not easy to classify the cyber crime. There are various modes and manner by with the cyber crime can be committed. Even the traditional crime is goingto be committed by using the computer or internet. The concept ofcrime 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 of illegal act, Thus the cyber crime can be classified on the basis of victims in the manner as following

4.1 Crime affecting Individual

4.2 Crime affecting economy

4.3 Crime affecting national security

a) Crime affecting Individual

Cyber crime has started to take place by this kind. Maximum cyber crimes are committed 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 gets access to the computer or account of the other and uses the private access by violating the privacy right of the victim. The computer is a common and important source of preserving personal data or information. Internet and the computer develop the techniques to restore the huge data of person in minimum time. Due to the capacity and the easy manner, this technique is going to use in everywhere from school to hospital and business enterprises to governmental and nongovernmental banking also make use or abuse of it<sup>11</sup>.

Internet and computer in business is called 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, less expensive process attracted the traders and businessperson to use this

mode for transferring the huge amount of

---

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



WHITE BLACK  
LEGAL

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 easier way to commit the criminal activities. The criminal activity as like hacking and IP spoofing are 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 commit conventional 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 nation at large are called cyber crime against the national security. Nowa 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 telecommunication and 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, and to communicate message among themselves to execute a plan. <sup>12</sup> Cyber warfare is another mode to commit the cyber crime which affect the national security. Computer and internet is

---



<sup>12</sup> Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 48.



WHITE BLACK  
LEGAL

integral part of military strategies of various countries in the world. 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 the world 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 touse. The computer crime and cyber crime are literally different but that cannot separate from each other by the legal system. Therefore, it is not easy to classify the cyber crime. There are various modes and 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

#### **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 with all 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 various provision from the enactment of the Indian Penal Code.

After coming into force of the Information Technology Act, 2000 on 17<sup>th</sup> 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 quite different therefore the amendments are required 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 discuss in the following ways;

**Similar offences also fall under the Indian Penal Code.**

(i) Sending threatening messages by email

Section 503 IPC



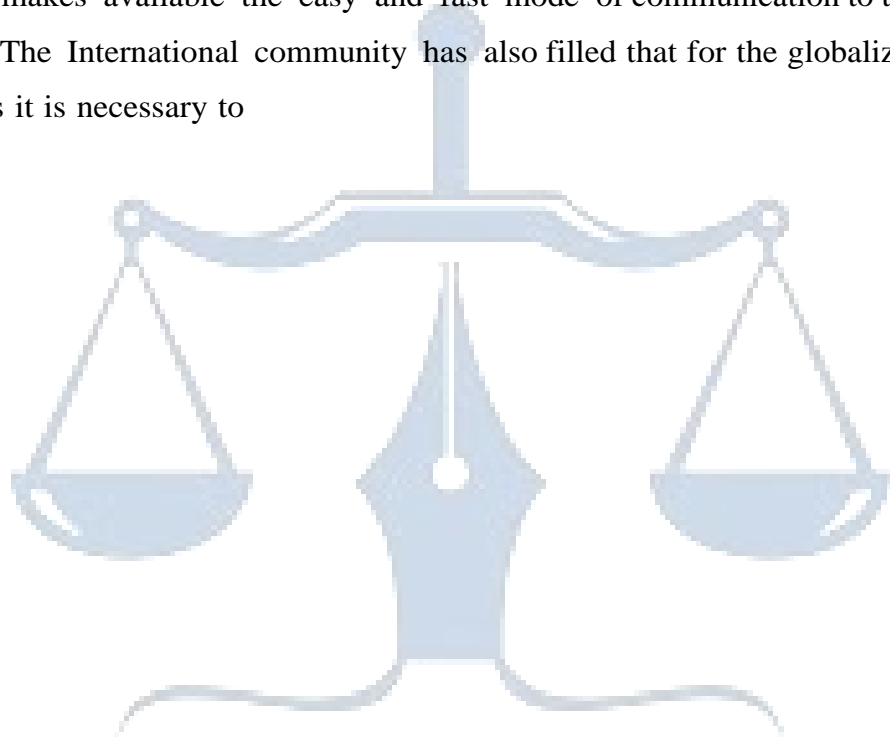
WHITE BLACK  
LEGAL

- (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
- (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 the 1999, 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 business community. The internet makes available the easy and fast mode of communication to the business world. The International community has also filled that for the globalization of the business it is necessary to



WHITE BLACK  
LEGAL

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 any law, then it is the duty of the legal system to enact the laws to protect from that act. Criminal law is the most important branch of the law, which is closely connected with everyone. It is rightly said that criminal law is the best when it criminalizes least. Therefore, when the cyber crime ramped in the society, it needs the effective criminal law to curb it.

The Information technology has invented the new world of cyber space. This world is the creation of the 21<sup>st</sup> 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 the duty of the state to protect the citizens in cyber space also. Therefore, it is necessary to the legal system to regulate the 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 with the 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 committed in 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 of internet. 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 are only a medium for storage, analysis and communication of information, communication that is fast outmoding or even replacing more traditional method of 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.”<sup>13</sup> Space perceived as such by an observer 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 pace with the rapid growth of the internet and its impact throughout the world. In spite of the recent fluency of legislation world-wide, it is unlikely that courts and legislators will be able to provide sufficient guidance in a timely fashion to business to enable them to engage in commerce or otherwise take advantage of the internet in a manner that avoids or minimizes 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 in which 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,

---

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



WHITE BLACK  
LEGAL

Further challenges are presented by the need for security in electronic network. Government is in favor 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, India too 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 also it facing the problem of the traditional notion of the jurisdiction which is the great difficulty for the laws 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 contributing the 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 there under.<sup>14</sup>



WHITE BLACK  
LEGAL

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 privacy as 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 Indian legal system require the law relating to the computer and Internet therefore the Information Technology Act and certain special rules enacted by the Indian legal system. Due to certain technical nature, certain amendments also need therefore the Indian Legal system formulated the rules to maintain its legal status in international family.

To meet the need of 21<sup>st</sup> 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 this Act, which involve the use of alternatives to the paper base means of communication and storage of information, to facilitate the electronic filing with the government agencies. Along with the enactment of the IT Act 2000, to recognize the electronic 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 30<sup>th</sup> January, 1997, as

well on the Model Law on Electronic Commerce.<sup>15</sup>

as UNICITRAL This

is only one act in Indian legal system, which known as the Cyber Law of India.

---

<sup>15</sup> IT Act 2000 vs 2008- Implementation, Challenges, and the role of adjudicating officers. By Karnika seth



WHITE BLACK  
LEGAL

and the recognition of the digital signature. As K.P. Singh has rightly pointed out the major issue covered under the provision of the act are as following<sup>16</sup>.

- a) Establish rules which recognize and validate contracts and execution through electronic mediums;
- b) Recognizes the admission of computer evidence in courts and arbitration proceedings

The law is enacted to meet the digital technology and new communication technology and it also provides penalties for misuse or illegal use of technology in 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 for bringing 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 offences and penalties. Chapter XI of the act deals with offences and the Chapter IX deals with penalties and the authorities regarding adjudication. These two chapters of the I.T. act deals with certain cyber crimes. Chapter IX focus on the following important features:

- a) Regulating conduct in its unique way;

---

<sup>16</sup> Laws on Cyber Crime: P.K.Singh (2007), Book Enclave, Jaipur, First Publication.

Page 96.



WHITE BLACK  
LEGAL



- b) Civil regulations to be employed by premise rather than criminal;
- c)The process of adjudication is entrusted to adjudicating officers rather than regular civil courts;
- d) Such adjudicating officers are required to know the laws and the IT or must have judicial experience;
- e) Adjudicating officers are vested with power of civil court;
- f) The proceeding to be conducted by such adjudicating officers are to be construed as judicial proceedings;
- g) The quantum of compensation to be calculated at market rate for loss 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 Act which deals with the civil liability, and if the act is comes under any penal provision of Criminal law, then it can registered under that Laws also.

Chapter XI of the Act defines certain offences and prescribed the punishment for that cyber crimes. For example, Section 65 of the Act deals with the offence of 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 extended up to two lakh rupees or both

---

<sup>17</sup> Section 65, The Indian Information Technology Act , 2000



WHITE BLACK  
LEGAL

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 of the



WHITE BLACK  
LEGAL

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

This section enacted mainly to protect the institution where the important data is going to be kept or stored. The most important step, which an organization should take 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 easy to pin down the culprit.<sup>51</sup>

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 computer resource. In the language of the computer, it is called hacking. The act in this offence is going to be committed by using the dishonest intention.<sup>18</sup>

---

<sup>18</sup> Cyber Law & Crime : Barkha U Rama Mohan (2011) Asia Law House, Hyderabad.



WHITE BLACK  
LEGAL

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 place in 2008, which has changed the nature of the

I.T. Act. To meet the hurdles for the enforcement certain important sections are inserted in the I T Act and it brought the various illegal activities 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 preview of 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 brought the service providers under the purview of cyber crime. The amendment Act also inserted various new things in the Act as like the controlling



WHITE BLACK  
LEGAL

authority, power of adjudicative authority. However, more important is that, certain provisions regarding the offences are included in the Act.

### **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 provisions in 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 be violated by different mode so it requires to be in the Act. A new offence of Cyber terrorism is added in Section 66 F which prescribes punishment that may 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 offences against 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 for cyber criminals. Further, as per new



WHITE BLACK  
LEGAL

Section 84B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new Section 84C makes attempt to commit an offence also a punishable offence with imprisonment 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 five years 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 on subsequent 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 act or 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.

WHITE BLACK

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 person who 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, because the 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 orin certain crime it is target.<sup>19</sup>

## 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 cyber crime is 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.

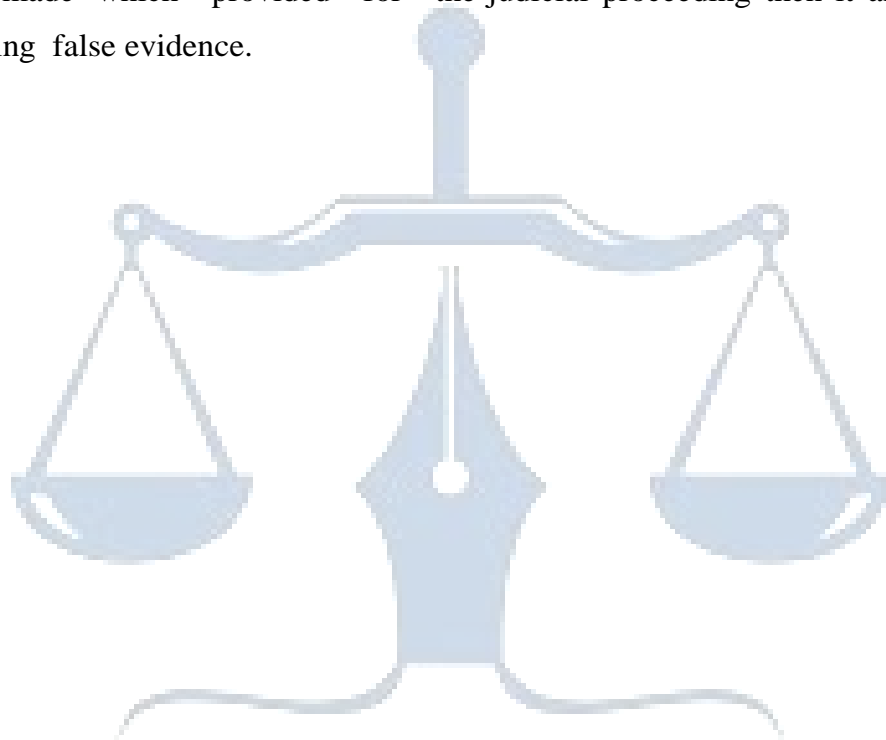
Therefore the enactment of Information technology compel the law makers to amend the Indian Penal code, which is called as a conventional Penal law of India. The First schedule to the Information Technology Act of 2000 has amended the certain provisions of Indian Penal code, 1860. The amended provision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

Sec. 192 of the Indian Penal code has amended the meaning of

---

<sup>19</sup> [http://catindia.gov.in/writereaddata/ev\\_rvnrbv111912012.pdf](http://catindia.gov.in/writereaddata/ev_rvnrbv111912012.pdf) last access on dated APRIL 2023at9.21pm.

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, then most 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 false evidence, whenever any electronic record is falsely made which provided for the judicial proceeding then it amount to be fabricating false evidence.



WHITE BLACK  
LEGAL

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 to that 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 threatening 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 in the offence provided under section 416 of I.P.C. that is cheating by personation. Apart from this various 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 comes under 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 were made in the Indian Penal Code in 2008. The amendments were sought to bring the paperless transactions under the purview 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 records and documents because substantive as well as procedural law, Indian Penal Code, 1860, Indian Evidence Act, 1872 and even Criminal Procedure Code.

In the Indian Penal Code the certain words as like 'computer resources' or 'electronic record' are inserted in various sections as like section 119, 167, 173, 175 etc. 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 354A stalking, these offences are 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 woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- (ii) Monitors the use by a woman of the internet, email or any other form

of electronic communication, commits the offence of stalking.



WHITE BLACK  
LEGAL

Provided that such conduct shall not amount to stalking if the man who pursued it 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 requirement imposed by any person under any law; or
- (iii) In the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, 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 Penal 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 cyber criminal towards the victim by using Internet services. Stalking in General



terms can be referred to as the repeated acts



WHITE BLACK  
LEGAL

of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victim's pet, vandalizing victim's property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends 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 domain name in connection with the sale 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 expenses.

(c) Data Diddling

This kind of attack involves altering the raw data just before a computer processes 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 is designed to injure a person'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 what it 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.



WHITE BLACK  
LEGAL

(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 such crimes take place, both laws can be attracted. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

(h) Internet time theft

It is nothing but one kind of cheating, where the internet is a tool for committing this crime. This crime 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 itself 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 themselves and 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 a cyber 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 has actually been sent from another source. Such kind of



WHITE BLACK  
LEGAL

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 vary from individuals to companies and even the email service provider. This is one 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 crime are the financial institutions. This attack has a unique quality that the alteration is so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program whereby

ameager sum of Rs 3 is deducted from custom account Such a  
ers .

small amount will not be noticeable at all. However, due  
r,

such merger from all the account holders collect huge amount.

This is purely a criminal 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 loses 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 is one kind of hacking, but the IT Act has not used the word hacking specially, but deals with the various kinds of unauthorized access or tampering with the computer resources, IT Act cannot cover all kinds of hacking therefore IPC is generally applicable to such kind of the unauthorized access.



WHITE BLACK  
LEGAL

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 of the 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 are dealing with the procedure of criminal proceeding. Due to increasing crimes of fraud through the computer and internet, these Act are also required to amend and make suitable for the information technology age. Considering the need required 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 2008. 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.

In Criminal Procedure Code, after Section 198 A<sup>20</sup>, 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 a complaint 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 shows that India is successful in facing new challenges of IT. Many amendments have been made in the Copy Right Act on the argument



---

<sup>20</sup> Section 198 A of Cr. P.C. 1973



WHITE BLACK  
LEGAL

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.**

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 laws are relevant in certain misuse in cyber space. However, generally the fraud is there in cyber 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 and internet. 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.



WHITE BLACK  
LEGAL

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 problem in 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 transnational jurisdiction, but execution is possible when all countries in the world recognized that act as a crime, and allow the proceeding on that aspect.



WHITE BLACK  
LEGAL

## CHAPTER-III INVESTIGATION IN CYBER CRIME

### **Introduction**

In criminal matters, there are different stages of criminal proceeding. Inquiry and trial are the stages where the courts are concerned. Inquiry, which is a much wider term, so far as the trial is concerned regarding crime only, but inquiry deals with any act whether it is crime or not, in other words after completion of inquiry, trial begins of those acts which are crimes. However, the inquiry and trial can take place whenever investigation is completed. The Investigation, inquiry and Trial are three different stages of criminal proceeding. The first stage is investigation, in which when Police get information of any crime, subject to the order of magistrates or without order of magistrates, brings the criminal law in operation to find out the truth, investigation is starting point of criminal law, its effectiveness needed for implementation of any criminal law.

There cannot be a uniform process of investigation. The investigation officer has to apply different techniques while investigation of any crime. Investigation is a skill and therefore it requires a special knowledge regarding the subject matter, in which the investigation officer is investigating. Offences whether conventional or the cyber crime, the same things are required that is nothing but the techniques. In case of offences where the offenders use special tools, that can be investigated by using the special techniques and expertise in that subject.

The Code of Criminal Procedure provides the general procedure for investigation of the crime. The conventional crime is investigated by using the regular methods. The law enforcement agencies were bound by some

basic rules and procedural aspect. There were established procedures for investigation and prosecution of all types of crimes. In case of traditional crimes, various physical evidences are generally available on the place of crime, collection of such physical evidence required a lot of common sense and little technical knowledge.

In cyber crime investigation certain special skill and scientific tools are require without which investigation is not possible. The Indian legal system introduced certain special provisions while investigating the cyber crime. The Information Technology Act, 2000 has bound to amend certain provision of Criminal Procedure Code and the Evidence Act. Along with this, certain new regulation has enacted by the Indian legal system to meet with the need of cyber crime investigation.

### **3.1 Investigation**

The word investigation derived from the Latin word “investigation” which means “to trace out or to search into” means nothing but find out the truth. The duty of investigation officer is not only limited to the collection of evidence on the basis of which, conviction may be secured but to bring out the real unvarnished truth. The investigation in simple is nothing but to bring the truth along with the evidences. It is first step while executing the criminal law in any matter.

When any information regarding crime given to the police, then what stages police takes, is call investigation. It is nothing but collecting evidences regarding the incidents, which takes place. According to Criminal Procedure Code clause (h) of section 2, Investigation includes all the proceedings under the code for collection of evidence conducted by police officers or by any person other than magistrate who is authorized by the magistrate.

The Madras High Court has considered the term investigation in extenso<sup>21</sup>.

---

<sup>21</sup>

<sup>21</sup> *Jumuna V. State of Bihar*, (1974) 3 SCC 774



WHITE BLACK  
LEGAL

The Supreme Court, while construing the term investigation has observed that under the code, “investigation” generally of the following steps *viz.*

- (1) Proceed to the spot.
- (2) Ascertaining all the facts and circumstances of the case,
- (3) Discovery and arrest of suspected offenders,
- (4) Collections of evidence relating to commission of offence, which may consist of
  - (a) the examination of various persons (Including the accuse) and the reduction of their statements in writing, if the officer thinks fit,
  - (b) the search of place or seizer of things considering necessary for the investigation and to be produced at the trial, and
- (5) Formation of opinion as to whether on the materials collection, there is case to place before the magistrate for the trial and if so, taking the necessary steps for the same by filling the charge-sheet under section 173.

Section 157 of the code provides the procedure for investigation. When the officer-in-charge of police station suspects the commission of an offence, from statement of First Information report or on the magistrate directs or otherwise, the officer or any subordinate officer is duty-bound to proceed to the spot to investigate facts and circumstances of the case and if necessary takes measures for the discovery and arrest of the offender. It primarily consists of ascertaining facts and circumstances of the case. It includes all the efforts of a police officer for collection of evidence: proceeding to the spot. Investigation includes the ascertaining of facts and circumstances along

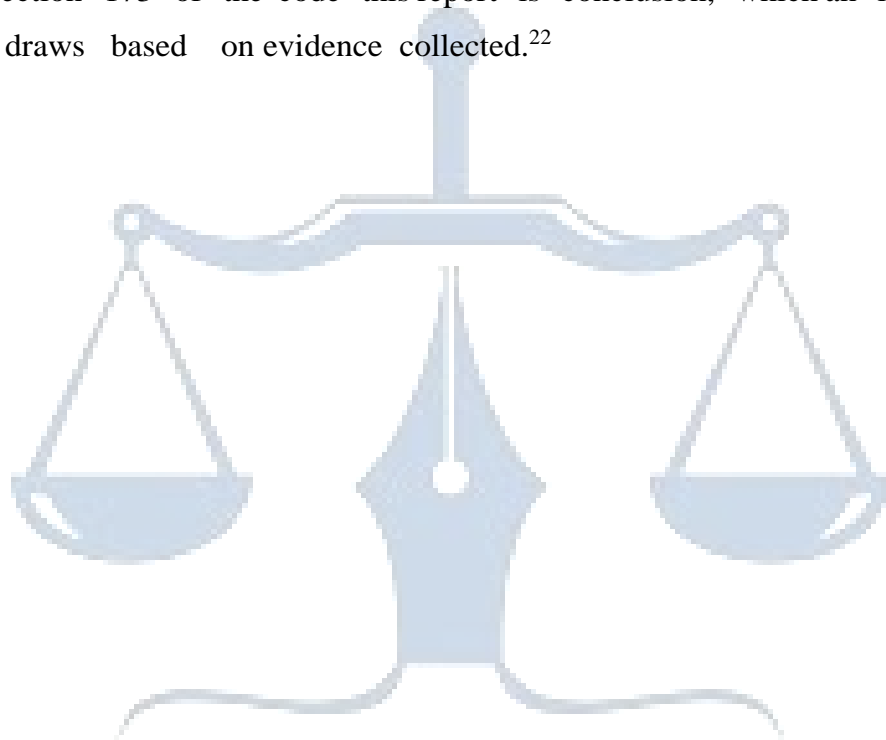


discovery and arrest of the suspected offender. It is collection of evidence relating to the commission of offence.



WHITE BLACK  
LEGAL

It may consist of the examination of various persons including the accused and taking of their statements in writing and the search of places or seizure of things considered necessary for the investigation and to be produced at the trial. It is formation of opinion as to whether on the basis of the material, collected there is a case to place the accused before a magistrate for trial and if so, taking the necessary steps for filing the charge-sheet. The investigation ends with submission of a police report to the magistrate under section 173 of the code this report is conclusion, which an investigation officer draws based on evidence collected.<sup>22</sup>



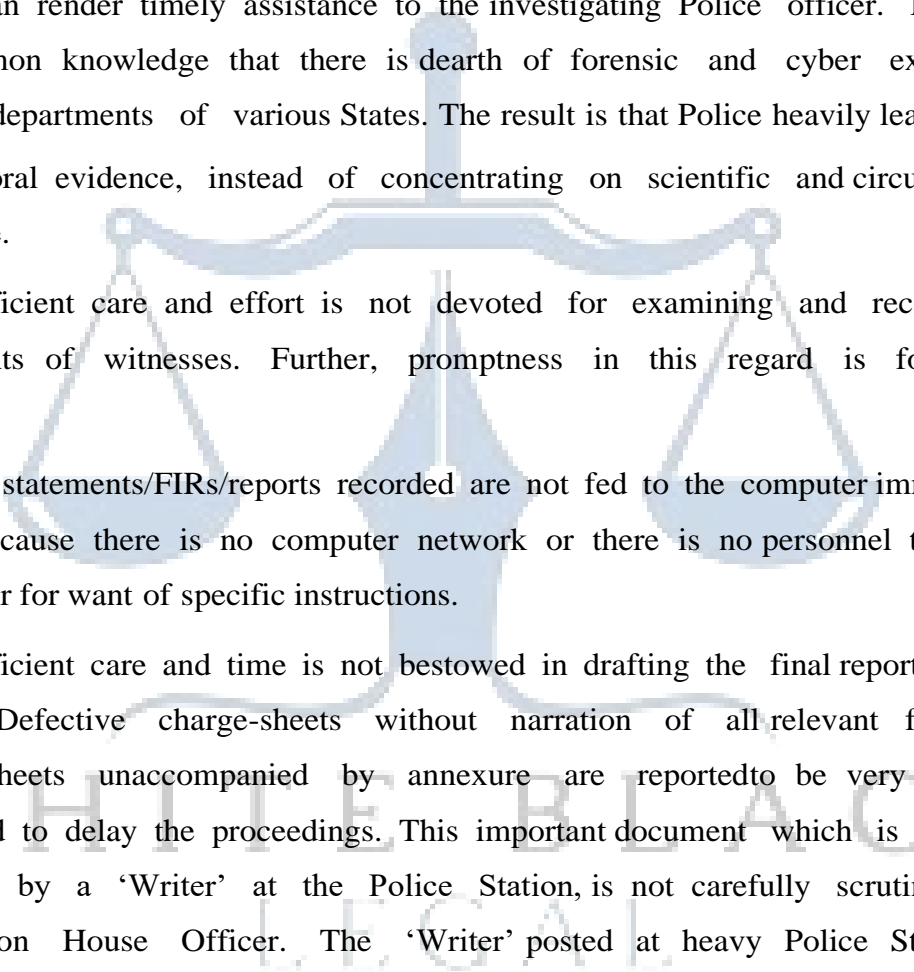
WHITE BLACK  
LEGAL

---

<sup>22</sup> <http://www.lawteacher.net/administrative-law/essays/administration-of-criminal-justice-law-essays.php#ft>last access on dated APRIL 2023 at at 7.00

WHITE BLACK  
LEGAL

While doing investigation generally the police require various things, however the requiring this are lacking in regular investigation as like;

- 
- (i) Police are quite often handicapped in undertaking effective investigation for want of modern gadgets such as cameras, video equipment etc. Forensic science laboratories are scarce and even at the district level; there is no lab, which can render timely assistance to the investigating Police officer. Further, it is common knowledge that there is dearth of forensic and cyber experts in police departments of various States. The result is that Police heavily lean towards oral evidence, instead of concentrating on scientific and circumstantial evidence.
  - (ii) Sufficient care and effort is not devoted for examining and recording the statements of witnesses. Further, promptness in this regard is found to be wanting.
  - (iii) The statements/FIRs/reports recorded are not fed to the computer immediately either because there is no computer network or there is no personnel trained in the job or for want of specific instructions.
  - (iv) Sufficient care and time is not bestowed in drafting the final reports/charge-sheets. Defective charge-sheets without narration of all relevant facts and charge-sheets unaccompanied by annexure are reported to be very common and tend to delay the proceedings. This important document which is normally prepared by a 'Writer' at the Police Station, is not carefully scrutinized by the Station House Officer. The 'Writer' posted at heavy Police Stations is overworked and can hardly spare the needed time.
  - (v) The photographs of accused (not to speak of witnesses) are not affixed to the charge-sheets/arrest Memos etc. nor even the identification marks are noted, making it difficult to identify the accused in the course of trial or to trace the absconding accused.

The purpose of criminal investigation is to find out the truth or

otherwise of the allegation made in the first information report and consequently Courts have no jurisdiction or authority to inquire into the allegation made in the first information report for quashing the same. On completion of the investigation, a charge-sheet is submitted, competent court may take cognizance of an offence if disclosed by the material collected during the investigation and it is only when cognizance is taken that the court gets the jurisdiction to decide on the merits' of the cases of the respective parts. The investigation can be quashed on that ground alone as any case of mala fides made out against the investigation agency.

The crimes, therefore the Police investigation is also require certain development in its working, and require to develop certain technology in every aspect. Due to the information technology development, generally all the governmental offices working is turn towards the paperless working. In comparison with other departments of the government, Police department is still following the age-old way of official working. Recently some development takes place, and Indian Police system has introduce certain technological development to reduce the paper work in the official working.

### **3.1.1 Information Technology and Investigation machineries;**

The Indian investigation machineries still following the traditional tools for the investigation. Due to the traditional way of investigation, the conviction rate is quite low in India. The police system is still requiring much development in its working. Though in 1980 and subsequently certain development takes place. Police and the crime investigation is the subject matter of the state. Maharashtra government has introduced various developments in the department. It has created various new branches and introduced the commission head in the metro cities. Apart from this, the police department has tried to develop its working by using the information technology. In order to make use of information technology Maharashtra police implemented the computerized

system called CIPA at police station and CCIS as districts. This project introduced the information technology in the police system. Now the various regular working of the police station are carried by using the information technology of the computer.

In order to make use of information technology Maharashtra police implemented the computerized system called CIPA at police station and CCIS as districts.

#### A. Common Integrated Police Application [CIPA]

CIPA is aimed at building the basic infrastructure and mechanisms for the Crime and Criminal Information System, based on Cr P C, which is uniform across the country, from Police Station level onwards. CIPA being a National project is to be implemented in a time-bound manner from police station level onwards for computerization of police records and use of IT in their functioning on a uniform basis throughout the country.

The national level Central CIPA Implementation Committee comprising of Director, NCRB and representatives from the Ministry of Home Affairs (Police Modernization and Union Territories Divisions), NIC (National Institute of Criminology) and Forensic Science and States, has been constituted to monitor the implementation. State Crime Records Bureau and State Police Training Academies are conducting State Specific courses in this connection with the assistance of NIC. NCRB has introduced two advanced courses on CIPA in its training calendar for resource persons, who in turn will impart training and attend to trouble-shooting in the States.

#### B. Crime Criminal Information System [CCIS]

In order to make use of Information Technology the Government of India has designed Crime Criminal Information System [CCIS] to store and retrieve crime and criminal records. This system has been upgraded to CCIS

Multi-Lingual web-enabled(CCIS MLe) in the year 2005 with facility for 5 regional languages i.e. Marathi, Gujarati, Tamil, Kannada and Gurmukhi, besides English and Hindi. Feature of crime analysis through data warehousing has also been added. The application has been web-enabled so that the field level investigating and supervisory officers can access the CCIS MLe database at National and State Levels through internet; anywhere - anytime.

Apart from this the other projects are introduced in Maharashtra with intent to enhance the use of information technology in the working of police and investigation process<sup>23</sup>. As like POLNET and the FPB (Finger Print Bureau) are another project which increased the use of information technology. This is the technological development in the investigation machinery, Maharashtra is an example so far as this development introduced in the Police system, considering this, some other state of India has also introduced it in the working of the Police. To investigate the crime is power of police, or the executive powers are concentrated to the police, now important aspect is to see, how the police can use their power and investigate the crime. Initially the technology was not so developed. The investigation is a process, where in the investigator has to apply his mind to find out the truth. The investigator

cannot rely on any specific way, he has to apply the different techniques not always scientific, but as per the situation apply his mind and bring out the truth in a process. Along with the development, the legal system tries to provide certain technical assistant to the investigation machinery by introducing certain special technical branches as like finger print expert etc. Such kind of technology are require in the present days. But yet the investigation machinery is quite less expert in comparison with the techniques which are going to be used by the criminals, therefore the impact of this can be seen in

---

<sup>23</sup> Prof. Hanmant N Renushe et al, Int. J. on Computer Technology & Applications, Vol.



WHITE BLACK  
LEGAL



investigation of technical offences as like the cyber crime.

#### **4.1 Investigation in cyber crime**

In legal system execution of law is depend on the executive. The criminal law can execute when the effective investigative machineries are available. In India, the legal system provide the machineries for investigation, along with the development, various new wings for investigation are established in India. However, cyber crime investigation is in need to find, to be developing, to tackle it effectively. The legal and judicial systems of India also need to adopt as per the contemporary information technology oriented society. However, a majority of cyber crimes in India has not reported due to ignorance. Even if some cyber crimes had reported, but they are not properly investigated and very few such cyber crime cases reach to the court for trial.

In the absence of scientific evidence and knowledge and proper cyber crime investigation, there are very few cyber crimes convictions in India. In fact, the Supreme Court of India is hearing many Public Interest Litigations (PILs) in this regard. <sup>24</sup>Today, with the advancement of technology, crimes have become more complex and criminals more sophisticated, as their modus operandi is incomparable to the traditional investigation methods. Information technology provides an opportunity to the criminals to commit traditional crimes like cheating, fraud, theft, credit card frauds, embezzlement of bank deposits, industrial and political espionage, cyber terrorism etc. and at the same time it helps in committing nontraditional and information technology related crimes like attacks against the security of critical infrastructures like telecommunication, banking and emergency services. Such crimes may be committed through computer networks across the national borders, affecting not only individuals, but they may instead result in compromising the security and the economy of the nation.

---

<sup>24</sup><http://cyberforensicsofindia.blogspot.in/2013/03/regulations-and-guidelines->

for.html last access on dated APRIL 2023 .at about 1.00 pm



WHITE BLACK  
LEGAL

The unique feature of cyber crime has rendered the traditional procedural laws as archaic and unsuccessful in resulting into conviction. The problems are not associated with procedure of the trial but also to extent of investigation and collection of evidence. The traditional rules and procedures of investigation and evidence collection are often of no use in the investigation of cyber crime. The criminal offence is committed in one country and extent to the other country and even to several another countries. The speed and accuracy is also very fast and perfect. The characteristics of cyber crime have raised a several issue and implication in the pre- trial investigation of cyber crime. 01The task of investigation agency is much challenging which include prevention of crime, collection of evidence, production of evidence before the court , arrest of accuse, security of system etc.<sup>25</sup>

Computer crime requires adequate expertise for investigation by expert investigating officers. So, the collection of evidence and the investigation should be made by an investigation team to carry out computer crime investigation with personal skill and experience

## WHITE BLACK

In India, cyber crime investigation is done by the superior offices of the police. The Information Technology Act 2000 set up a special procedure for investigation and further proceeding in cyber crime contended in the IT Act, 2000, which makes cyber crime investigation slow. Under section 78 of the Act, an Inspector shall investigate the cyber crime. Before the Amendment of 2008 in IT Act, the power of investigation was confer on the Deputy Superintendent of Police; the object behind this amendment is to bring the cyber crime for investigation in mainstream as

---

<sup>25</sup> Laws on cyber crime: P.K.Singh (2007), Book Enclava Jaipur, Page 131.



WHITE BLACK  
LEGAL

like a conventional crime. This Amendment gives power to the inspector to register and investigate the cyber crime as like another crime.

### **3.2 Investigation of cyber crime and challenges**

#### **3.3.1 Jurisdiction and problem**

The legal system is based on the notion of jurisdiction. Jurisdiction is an important notion while execution of any law in any country. The legal notion of jurisdiction helps to define and determine the power of state to regulate people, property and circumstances. This jurisdictional power confers the legal power to the state to make the laws means legislative power, implement the laws means the execution and adjudication means judicial powers. These all things can perform by the state when it has jurisdiction on the thing or act. Jurisdiction is of two kinds that are territorial and personal.

In case of traditional law and its enforcement, the notion of jurisdiction is not much complex, it is easy to the state to execute the law because it can execute by way of territorial jurisdiction or either personal jurisdiction. Jurisdiction is an important aspect because without having legal jurisdiction the investigation agency cannot exercise the power to investigate the matter. While doing investigation, investigation agency has to perform various things as like search and seizure, arrest and various other things. Therefore, the aspect of jurisdiction is most important in every investigation.

Since national boundaries effectively disappear when considering many computer

crimes, jurisdiction is another complicated matter. While a complete examination of jurisdictional issues is beyond the scope of this



WHITE BLACK  
LEGAL

work, it merits comment that countries differ in civil and criminal offences standards, substantive and procedural law, data collection and preservation practices, and other evidentiary and juridical factors. Moreover, it is often ambiguous as to whose responsibility it is to address a particular crime or spearhead an investigation, or how best to collaborate through extradition and mutual assistance policies. This plays out not only on an international level, but also within nations where multiple law enforcement departments are implicated.

However, the explosion of internet has created significant challenges for the traditional notion of territoriality and other established jurisdictional principles. The nature of cyber crime is different than the conventional crime. Basically the mode of committing the cyber crime is different, for cyber crime physical presence of the accused is not required at the place of crime. Due to this nature the traditional notion of jurisdiction is required to be changed. The traditional notion of jurisdiction is based on territorial theory and physical presence theory. The territorial theory protects the territorial integrity of the state, it empowers to investigate and inquire any crime within the territory of the said state. In physical presence theory, a presence of the person or property in a state is a basic ground upon which a legal authority exercises its jurisdiction over an accused. But cyber crime is quite different therefore both these theories can be useless in certain situations.

#### **4.3.1 Impact of the internet upon the territorial notions of jurisdiction:**

Introduction of new technology and in particular the internet has brought about important change to the way people interact and conduct in the society. In the famous *Burger Kings case*, a U S Court observed that

:

It is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire

communication across State lines, thus obviating the need for physical presence within a state in which a business is conducted.

The emergence of the internet based activities has challenged above mentioned foundation of traditional jurisdiction. Internet communications cut across state boundaries creating a new realm of human activities and weakening the legitimacy of applying laws based on territorial borders<sup>26</sup>. Some territorially-based law makers and law enforcements authorities find this new environment threatening. A state is territorial in nature while the internet has no strict relation to territorial boundaries. For example, a website can generally be viewed by any one (with access to a computer and modem), at any time, in any part of the globe. This tends to make the location of the site less relevant but broadens the geographic reach of a business.

Cyber space radically undermines the relationship between legally significant (but on line) Phenomena and physical location. The rise of the global computer network is eroding the link between geographical location and the following:

1. The power of local governments to assert control over online behavior;
2. The effects of online behaviors on persons or property ;
3. The legitimacy of the efforts of a state to enforce rules applicable to global phenomena; and
4. The ability of physical location to give notice of which sets of rules apply ,

A state is territorial in nature while the internet has little or no relation

---



<sup>26</sup> Judicial Jurisdiction in the Transnational Cyberspace: Dr. Bimal Raut (2004) New Era LawPublication. Page 42.



WHITE BLACK  
LEGAL

to territorial boundaries. Investigation of any crime is start when the agency having jurisdiction. None of the traditional theories underpinning the notion of jurisdiction, The traditional theories of jurisdiction are inapplicable to the internet because:

- Material posted on the internet have a world-wide audience;
- It is easy to move a website from one territory to another

[ A websit can be hosted in one area but directed a th  
e t e  
users in another geographic location:

- Part of the website may be hosted in one area while other pa  
rt  
of website are hosted in another location:  
the
- It is not always possible to determine whether a website or user is located.

Then the issue is that whether the global nature of internet can be the subject matter of the traditional notion of jurisdiction Though the procedural laws has provided certain clauses that can be use while investigating the cyber crime. Certain new provisions of the laws are useful but not effect as require in the present days.

The same issue was discussed in the High Level Consultation Meeting for formulation of a National Policy and Action Plan for Enforcement of Cyber law, at New Delhi on 31, Jan 2010. Where in Mrs.Karnika Seth has contended that major challenge in enforcement of cyber laws is posed by

the fact that there are no territorial boundaries in the Cyberspace and there are heterogeneous laws across the globe. A very radical and direct way to solve the question would be giving an entity supra-national powers on cybercrime matters, thereby abolishing borders and creating a single, global, cyber-jurisdiction. However, this seems to be



WHITE BLACK  
LEGAL

highly unrealistic and a virtual myth<sup>27</sup>.



WHITE BLACK  
LEGAL



---

<sup>27</sup> <http://www.karnikaseth.com/evolving-strategies-for-the-enforcement-of-cyberlaws.html> last access on dated 19/10/2015 at 9.30 pm.

Thus the starting point that jurisdiction is the main problem while investigating the cyber crime, and the same issue was a big hurdle in a famous case known “Love Bug”. Therefore, the legal system has to think regarding the problem of jurisdiction, without which investigation of cyber crime cannot be done effectively.

Considering the problem of jurisdiction the Criminal procedure code and IPC is amended at time of enactment of the Information Technology Act 2000, which has provided regarding the jurisdiction. Chapter XIII contains section 178-186 and the section 188 which are meant to enlarge the ambit of the “local Jurisdiction” in which the inquiry or trial of the offences might take place. Apart from dealing with the offences committed within India, the Cr .P. C. also supplements Section 4 IPC which contains the extension of the IPC to extraterritorial offences.

The amended Section gives jurisdiction to the Indian Court if the affected computer recourse is situated in India. The procedure to be followed is as given under section 188 Cr. P. C. and I T Act Section 2(I). The combined rules given under this section depict the legitimate right of a sovereign state on its citizens, not only on its lands but also beyond it, that is on any foreign land. Thus, the amendment somewhere tries to provide the jurisdiction, but the execution of this section is still not possible without the co-operation by the other State. Therefore, the International co-operation is the immediate need for resolving the problem of jurisdiction in case of the Cyber Crime investigation.

#### **4.3.2 Electronic/ Digital Evidences**

Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form. It can be stored or transmitted. It can

exist in the form of computer files, transmissions, logs,



WHITE BLACK  
LEGAL

metadata, or network data. Digital forensics is concerned with recovering – often volatile and easily contaminated – information that may have evidential value<sup>28</sup>. Forensics techniques include the creation of ‘bit-for-bit’ copies of stored and deleted information, ‘writeblocking’ in order to ensure that the original information is not changed, and cryptographic file ‘hashes’, or digital signatures, that can demonstrate changes in information. Almost all countries reported some digital forensics capacity. Many responding countries, across all regions, however, note insufficient numbers of forensic examiners, differences between capacity at federal and state level, lack of forensics tools, and backlogs due to overwhelming quantities of data for analysis. One-half of countries report that suspects make use of encryption, rendering access to this type of evidence difficult and time-consuming without the decryption key.

Indian evidence Act is applicable to civil and criminal cases. In cyber crime the evidence may be in any form including electronic or digital evidence. Digital evidence is any information stored or transmitted in digital form that a party to the case may use it in the trial. Whenever any digital evidence is going to submit in the court of law, before accepting it, Court will determine if the evidence is relevant, whether it is admissible. Court also determine, whether it is hearsay and whether a copy is acceptable or original is required.

In conventional crime, the evidences generally find on the spots of incidents but in case of electronic evidence, it can be find in digital photographs, e-mails, ATM transactions. Due to the enhancement in technology, various software’s developed, in every field. Initially the accounts are going to maintain in the hard copy or account books; now

---

<sup>28</sup> Cybercrime: Talat Fatima, (2011) Eastern Book Company Lucknow. Page 356.



account and calculation data can save from accounting program. Even now, electronic doors are invented, therefore in case of any incidents or offences the evidences any be available but in the digital form. Therefore, a computer forensics branch is comes into existence. The goal of computer forensic is to explain the current state of a digital artifact. Digital artifact includes hard disk or CD-ROM and JPEG. Considering the need the concept of evidence has undergone change and now this document in electronic form is recognize as evidence.

The Amendment in Evidence Act, 1872 bring the electronic document under the preview of evidence. The definition of documentary evidence has amended to include all documents including electronic record produced for inspection by the court. Section 3 of Indian Evidence Act, 1872 defines evidence as, Evidence means and includes 1) All statements which the court permit or require to made before it by witness in relation to matter of fact under inquiry; such statements are called oral evidence; 2) All documents including electronic records produced for the inspection of the court. Such documents are called documentary evidence. The term electronic record in evidence act and the term date in Information Technology Act is having same meaning.

For the admissibility of the electronic record the Amendment in Indian Evidence Act in the year 2000, includes certain new section as Section 65A and 65B and these sections provides that the contents of electronic records may be proved in the court of Law. Thus, the Indian Evidence Act, which is applicable to conventional crime and the cyber crime are considering in same manner, whether it is cyber crime or the conventional crime. Only due to the digital nature of the evidences, the rules of evidences are requiring to be change. The Section 17 of the Indian Evidence Act which deals with admission, now it include the statement in electronic form which suggest an inference to fact at issue or of relevancy. This amendment is made purely to create the validity to the digital evidence. New Section 22A has inserted in Indian Evidence Act,

1872 with intent to provide the relevancy of oral evidence regarding the content of electronic record. It provides that oral admissions regarding the contents of electronic record are not relevant unless the genuineness of the electronic records produced is in question.

Therefore, for the digital evidence is concern these two sections Section 65A and 65B are introduced in Indian evidence Act, for the relevancy of the electronic evidence in court proceeding. Section 65A provides that the contents of electronic record may be proved in accordance with the provisions of section 65B. Section 65B provides that notwithstanding anything contained in the Indian Evidence Act, 1872 any information contained in an electronic form is deemed to be a document and it admissible in evidence without further proof of the original's production provided that the condition set out in section 65B are satisfied.

To understand the scope of the section 65 B, all the clauses of this section are required to be seen, which provides how the evidence Act recognized the electronic evidence.

Sec. 65B (1): Notwithstanding anything contained in this Act, any information contained in an electronic record -<sup>29</sup>

- which is printed on a paper, stored, recorded or
- copied in optical or magnetic media
- produced by a computer
  
- shall be deemed to be also a document, if the conditions mentioned in this section are satisfied

- in relation to the information and

---

<sup>29</sup> Section 65B Indian Evidence Act, 1872



WHITE BLACK  
LEGAL

- computer in question and
- shall be admissible in any proceedings, without further proof or production of the original,
- as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

**Sec. 65B (2):**

The **computer** from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

**Information** was fed in computer in the ordinary course of the activities of the person having lawful control over the computer;

The **computer** was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

**Information** reproduced is such as is fed into computer in the ordinary course of activity.

**Sec.65B(3):**

The following computers shall constitute as single computer-

- by a combination of computers operating over that period; or
- by different computers operating in succession over that period; or

- by different combinations of computers operating in succession over that period; or



WHITE BLACK  
LEGAL

Cyber space is boundary less world, which cannot divide in particular countries or territories as like the physical world. Cyber space is subject matter of the users, because it available to anyone who is having access of the internet or computer. However, it is duty of legal system to protect the rights of their citizens in the cyber space. A safe and secure online environment enhances trust and confidence and contributes to a stable and productive community. In initial period the countries, which are having the more territory and the strong power to protect are known as powerful countries. However, now the position has undergone change. In this age of information technology the countries, which is having latest techniques about internet, are call the powerful country. Due to this situation, small countries got important position due to the techniques.

Information and communications technology (ICT) is an integral part of our daily lives. Whether people have a computer at home, use online banking services or simply receive electricity supplies, the community's reliance on technology is increasing. Government and business also take advantage of opportunities for economic development through increased use of information technology and a technology aware population with internet connections locally and overseas.

Cyber crime is not a national problem but it is a problem found all over the world. The international access to information and mobility of data is one of the most important functions of world economic system. One of the peculiar characters of the cyber crime is that its impact is very wider than the conventional crime .A criminal act committed in one part of the world may cause impact at some other part of the world. In view of reach of the cyber crime, entire world has virtually turned in to a small village. Another feature is that the criminalization increase in the cyber crime is uniform all around the world. The basic problem in the implementations of the cyber crime

in the global



WHITE BLACK  
LEGAL

perspective is that the act is crime in one country and not crime in another country, that create the basic problem, the same problem was faced in the famous case of 'love bug' case where in the citizen of the Philippines cannot be convicted. Now the enactment of the cyber law has resolve the said problem, now any person who committee crime anywhere and damage the computer of any counters, he can be held liable to the offence.

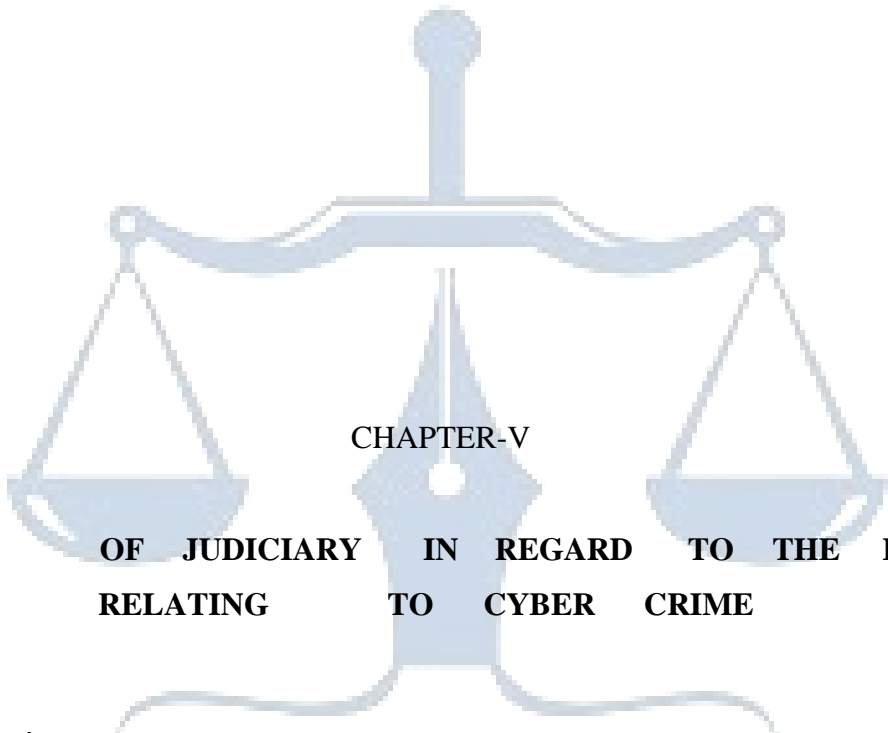
#### **4.1 Global perspective**

In present day's everyone is liable to promote a safe and reliable environment in cyberspace world, in the context of an emerging information society. The information technology is developed, due to development in the Information technology, the world becomes a global village, distance between the countries has drastically undergone change, and this technology allows easy access. The gift of the 20<sup>th</sup> century is the internet, which connected the entire world but along with easy access, internet provide easy way to the cyber criminals for committing the crime from any corner of the world. Thus, cyber crime has the omnipotent characteristics and therefore, it can have victims anywhere in the world. It is now essential that all those persons, who deals with cyber world, must have some idea about as to what acts constitute cybercrime in the different countries of the world. Therefore, the entire countries of the world have prepared the cyber laws as per their need and ability to execute it.

Since impact of cyber crime is unbounded, any effort made at national level have to meet international coverage of sake of effective containment of cyber crime and protecting the interest of the society. Such situation necessitates understanding of global legal response relating to the cyber crime. The discoveries and the inventions both constructive and destructive are very rapid all around the world. In absence of international cooperation, it will not be possible for any country to



know the recent advances in the other country.



CHAPTER-V

**ROLE OF JUDICIARY IN REGARD TO THE LAW  
RELATING TO CYBER CRIME**

**Introduction**

In every legal system, which accepts the democratic form of government, the Judiciary plays an important role. It is most important wing of the government, which resolves the conflicts among the parties. For the development of the society, the smooth and powerful adjudicative authority is required. The changing nature of the society increases the role of the adjudicatory authority in the present days. In the era of Information and technology, the criminals are using new technology to commit the crime. Therefore, appropriate judicial approach towards the technological offences is required for prevention of the crime. For the proper working of the judiciary the rules of jurisdiction plays an important role. The main problem that is going to face in case of cyber crime is concern

with the jurisdiction. India is a developing country..

In India, there is only one set of court, which administers national as well as state laws. The constitution has by Article 247, clothed

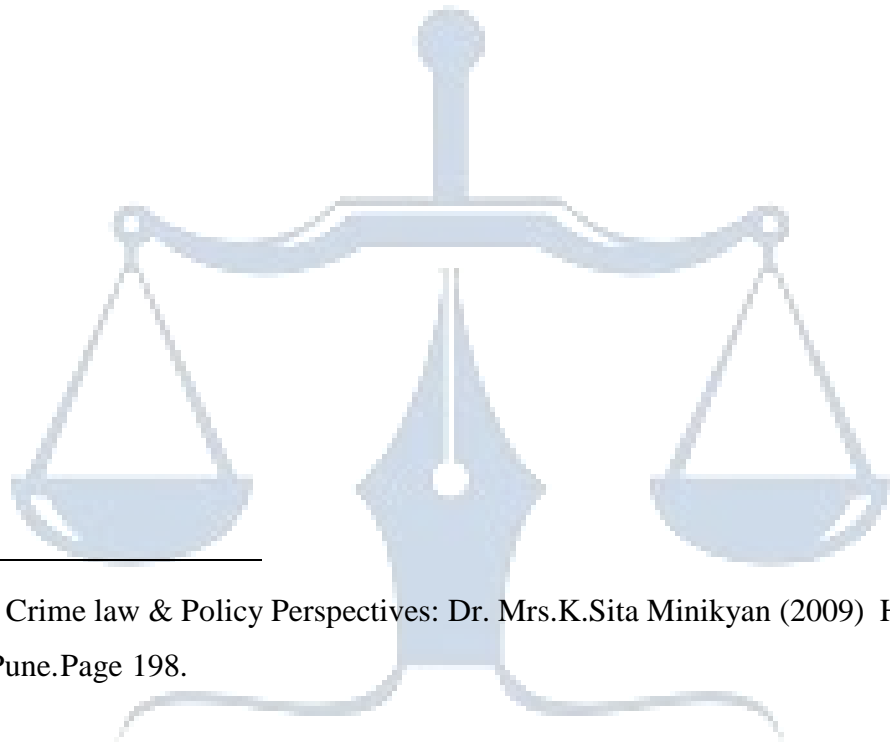


WHITE BLACK  
LEGAL

parliament with power to provide for the establishments of additional court for the better administration of law made by the parliament and of any existing law with respect to the matter enumerated in the union list. The courts in India are generally controlled by the state<sup>30</sup>.



WHITE BLACK  
LEGAL



---

<sup>30</sup> Cyber Crime law & Policy Perspectives: Dr. Mrs.K.Sita Minikyan (2009) Hind Law House Pune.Page 198.

WHITE BLACK  
LEGAL

Recently the Indian legal system has established certain tribunals, which deals with certain special matters as like the recovery of debt, or certain tribunals for Income tax etc, but lastly the all tribunals are subjects of the judicial review of High Court and Supreme Court. Therefore, the judiciary plays an important role in all laws. However the basic problem arise when the offences are of that nature which require the technical knowledge to understand the nature of the act whether it is an offence or not. Due to this nature of cyber crime, the legal system is facing various problems. The laws are insufficient but the policy and the operative system facing the difficulty of lack of knowledge. In case of judicial perspective, the basic question arising regarding the jurisdiction.

The conventional law as like Indian Penal Code and the procedural law that Code of Criminal Procedure has provide provisions regarding the territorial and extra territorial jurisdiction, but the basic nature of the cyber crime somewhere require something more than the provided rules therefore some reformations are required. If we see the decided cases on the cyber crime, we can find that whenever the provision of Information Technology Act, is attracted then along with that certain provisions of conventional criminal law, that is the Indian Penal Code is also attracted so it shows that the cyber crime is nothing but the expansion of the conventional law.

### **5.1 Court's Jurisdiction in Internet Disputes**

Jurisdiction is one of the debatable issues in the case of cyber crime dueto the universal nature of the cyber crime. The problem of jurisdiction is not only concern in investigation process but may arise in the trial proceeding also. With the ever-growing arm of the cyber space, the territorial concept seems to vanish. New Methods of dispute resolution should give way to the conventional methods. Thus, the Information Technology Act, 2000 is silent on

these issues.



WHITE BLACK  
LEGAL

Cyber Crime cannot be territorial but global because internet is network of networks as we have seen earlier. It has wide range of functioning; limiting it to physical boundaries is not possible. Thus even in case of cyber crime there might be a possibility where extra territorial jurisdiction arises.

Jurisdiction plays a vital role for undertaking a successful criminal procedure. Dealing with the issue of cyber crime it has been noted that even when investigating officer succeeds in establishing geographical identity of an accused of cyber crime, officer has to face many other difficulties in pursuing his investigation, such as an accused may fall beyond the jurisdictional powers of criminal justice system. In the cyber world where speed is an essence, any attempt to acquire such consent of courts or cooperation will thwart any chance of identifying the culprits and collecting evidence of the crime.

The Doctrine of ubiquity aims determining the place of commission. According to this doctrine, the offence will be considered to have been committed in its entirety within a country's jurisdiction, if one of the constituent elements of the offence or the ultimate result occurred within the country's territorial limit. Common Law countries also use effects doctrine in addition to focusing on the physical act. The doctrine locates crime in the territory where it intended to commit or actually took place. Territoriality might grant jurisdiction to many countries in single cyber crime.

Though S. 75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation's for exchange of material

and evidence of computer crimes between law enforcement agencies. evidence and its appreciation before the court. Apart from this, there is no difference between the cyber crime and the conventional crime.

## **CHAPTER-VI**

### **ROLE OF JUDICIARY IN REGARD TO THE LAW RELATING TO CYBERCRIME**

In every legal system, which accepts the democratic form of government, the Judiciary plays an important role. It is most important wing of the government, which resolves the conflicts among the parties. For the development of the society, the smooth and powerful adjudicative authority is required. The changing nature of the society increases the role of the adjudicatory authority in the present days.

In India, there is only one set of court, which administers national as well as state laws. The constitution has by Article 247, clothed parliament with power to provide for the establishments of additional court for the better administration of law made by the parliament and of any existing law with respect to the matter enumerated in the union list. The courts in India are generally controlled by the state<sup>31</sup>.

Recently the Indian legal system has established certain tribunals, which deals



with certain special matters as like the recovery of debt, or certain tribunals for Income tax etc, but lastly the all tribunals are subjects of

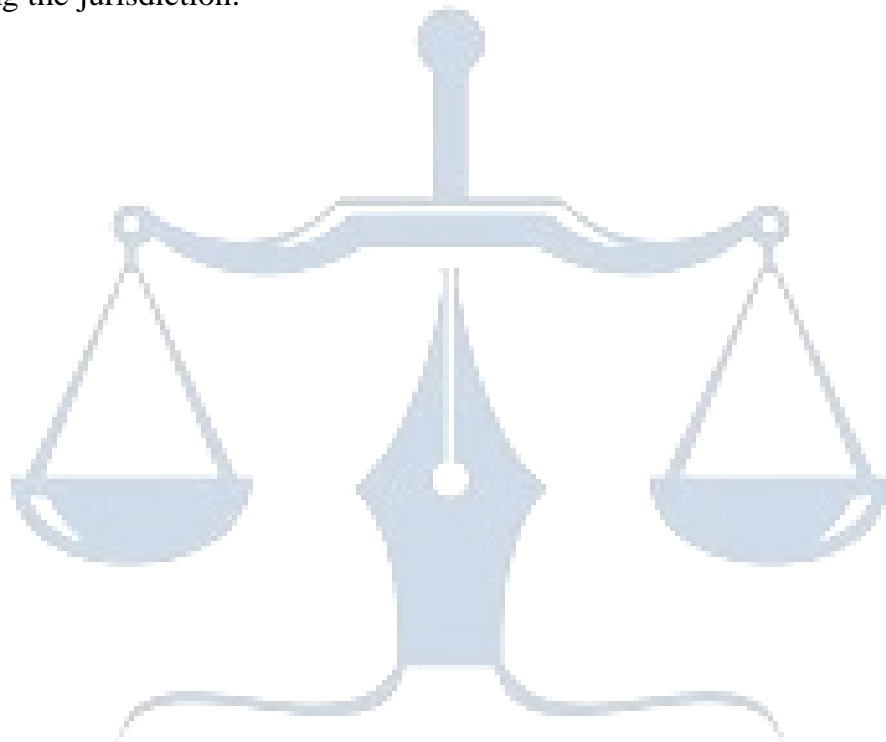
---

<sup>31</sup> Cyber Crime law & Policy Perspectives: Dr. Mrs.K.Sita Minikyan (2009) Hind Law House Pune.Page 198



WHITE BLACK  
LEGAL

the judicial review of High Court and Supreme Court. Therefore, the judiciary plays an important role in all laws. However the basic problem arise when the offences are of that nature which require the technical knowledge to understand the nature of the act whether it is an offence or not. Due to this nature of cyber crime, the legal system is facing various problems. The laws are insufficient but the policy and the operative system facing the difficulty of lack of knowledge. In case of judicial perspective, the basic question arising regarding the jurisdiction.



WHITE BLACK  
LEGAL

The conventional law as like Indian Penal Code and the procedural law that Code of Criminal Procedure has provide provisions regarding the territorial and extra territorial jurisdiction, but the basic nature of the cyber crime somewhere require something more than the provided rules therefore some reformations are required. If we see the decided cases on the cyber crime, we can find that whenever the provision of Information Technology Act, is attracted then along with that certain provisions of conventional criminal law, that is the Indian Penal Code is also attracted so it shows that the cyber crime is nothing but the expansion of the conventional law.

### **6.1 Court's Jurisdiction in Internet Disputes**

Jurisdiction is one of the debatable issues in the case of cyber crime dueto the universal nature of the cyber crime. The problem of jurisdiction is not only concern in investigation process but may arise in the trial proceeding also. With the ever-growing arm of the cyber space, the territorial concept seems to vanish. New Methods of dispute resolution should give way to the conventional methods. Thus, the Information Technology Act, 2000 is silent on these issues.

Cyber Crime cannot be territorial but global because internet is networkof networks as we have seen earlier. It has wide range of functioning, limiting it to physical boundaries is not possible. Thus even in case of cyber crime their might be a possibility where extra territorial jurisdiction arises.

Jurisdiction plays a vital role for undertaking a successful criminal procedure. Dealing with the issue of cyber crime it has been noted that even when investigating officer succeeds in establishing geographicalidentity of an accused of cyber crime, officer has to face many other difficulties in pursuing his investigation, such as an accused may fall

beyond the jurisdictional powers of criminal justice system. In the cyber world where speed is an essence, any attempt to acquire such consent of courts or cooperation will thwart any chance of identifying the culprits and collecting evidence of the crime.

The Doctrine of ubiquity aims determining the place of commission. According to this doctrine, the offence will be considered to have been committed in its entirety within a country's jurisdiction, if one of the constituent elements of the offence or the ultimate result occurred within the country's territorial limit. Common Law countries also use effects doctrine in addition to focusing on the physical act. The doctrine locates crime in the territory where it intended to commit or actually took place. Territoriality might grant jurisdiction to many countries in single cyber crime.

Though S. 75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation's for exchange of material and evidence of computer crimes between law enforcement agencies.

As we are known that internet is network of networks, and thus in the field of cyber space no activity is subject to any one particular jurisdiction. In such cases, territorial borders have no relevancy.

The current litigation system of India is not only antique in nature but has become cumbersome and time consuming as well. The backlog of cases is increasing day by day affecting the outcome of various cases. There is an emergent need of judicial and legal reforms in India so that courts in India

can meet the expectations of the 21st Century. This



WHITE BLACK  
LEGAL

can be done only by maintaining a stance that preserves the court's reputation and supports the court's critical role in maintaining public confidence in the protection afforded to them by the law. The Indian conventional laws are yet not suitable to deal with the correct issues, the laws regarding cyber law and Information Technology sector are far away from their real need. The Indian system already facing the problem of low conviction rate in all criminal matters, and the cyber crime and new technology has created many hurdles in the said aspect.

Indian Penal Code is universal criminal law of Indian legal system. However, it amended time to time, however its implementation is also not satisfactory in the view of people. The public confidence in the Criminal Justice System of India is declining and the same has forced the Government of India to bring this issue back to the top of the political agenda. Its aim is to cut crimes by increasing the number of criminals brought to trial and reducing the time taken to complete the legal process. Apart from that, the trial brings before the court, the appropriate appreciation of evidences and the conviction on that matter. Mere proper investigation is not sufficient but the proper appreciation of the evidences by the court is also necessary for the effective criminal justice system.

The Indian Legal system passed the Information Technology Act in 2000, the Act as contended previously is enacted for the regulation of e-commerce. However having certain penal provision but they are not sufficient to curtail the offences takes place by using computer as a tool or target. The various judgments of the Honorable

High Courts and the Hon'ble Supreme Court are prima facie based on the provisions of the traditional criminal law, i.e. Indian Penal Code.

These are various landmark cases, in which the issues are regarding the crime, which are subject to the use of computer or internet, though the offences are registered in different sections of the Information technology, and then it is subjected to the conventional criminal laws also, i.e. Indian Penal Code. The Judgments shows the effectiveness of the conventional criminal laws in the informational technology. Only the amendments in the procedural laws are necessary for the effective prevention of the cyber laws.

### **I. Anvar P.V. vs. P.K. Basheer and others**

In this significant judgment, the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.

The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance being placed on the audio-video recordings, which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD

are being forwarded without



WHITE BLACK  
LEGAL



a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

In the anticorruption cases launched by the CBI and anticorruption/Vigilance agencies of the State, even the original recordings which are recorded either in Digital Voice Recorders/mobile phones are not been preserved and thus, once the original recording is destroyed, there cannot be any question of issuing the certificate under Section 65B(4) of the Evidence Act. Therefore in such cases, neither CD/DVD containing such recordings are admissible and cannot be exhibited into evidence nor the oral testimony or expert opinion is admissible and as such, the recording/data in the CD/DVD's cannot become a sole basis for the conviction.

In the aforesaid Judgment, the Court has held that Section 65B of the Evidence Act being a 'not obstante clause' would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The Section 63 and Section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act. The Constitution Bench of the Supreme Court overruled the judgment laid down in the State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru [(2005) 11 SCC 600] by the two judge Bench of the Supreme Court. The court specifically observed that the Judgment of Navjot Sandhu supra, to the extent, the statement of the law on admissibility of electronic

evidence pertaining to electronic record of this Court, does not lay down correct position and required to be overruled.

The only options to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence in court or it's copy by way of secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

This case is important, which discuss in detail the admissibility of the digital evidence. The provisions regarding the digital evidence are discussed however, this judgment deals with the digital evidence and the admissibility of the digital evidence.

## **2. State of Tamil Nadu vs. Suhas Kutti,**

It was the first conviction case under the Information technology Act, 2000. Indian court firstly convicted for the offence of cyber crime. The judgment was pronounced in the year 2004, within the seven month after filing the FIR, which brings the conviction for the cyber crime. The Honorable Judge of the Additional Chief Metropolitan Magistrate has passed the order of conviction. In this case, the victim was a divorcee who constantly harassed by annoying phone calls presuming that she would solicit them because of a message posted on yahoo message group followed by forwarding emails. The message was extremely obscene, defamatory and annoying. The accused turned out to be her family friend and interested in marrying her.

The accused held guilty of offences under Section 469, 509 IPC and 67 of IT Act 2000. The accused had been convicted and sentenced for the offence to undergo RI for 2 years. Under section 469 IPC to pay fine of Rs.500/-and, for the offence u/s 509 IPC sentenced to undergo 1 year

Simple imprisonment and to pay fine of Rs.500/-, and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.

In the investigation of this offence, it is found that the main reason behind the act of accuse is to defame the reputation of the victim, therefore he use the way of internet and yahoo message. Due to this only the Information Technology Act is attracted, but this Act cannot cover the act intending of insulting the modesty of woman, and defamation therefore the Indian Penal Code is attracted. The investigation machineries use the information technology, where it found that accuse created user id in the name of her and composed an obscene message intending that such document shall be used for posting in different obscene Yahoo Group, with the intention to make others to believe that the document was made by her, so that the persons seeing the obscene message would send offending calls to her, in harming her reputation and by insulting her modesty by the words exhibited in the email and in the course of same transaction. The agency used to find out the I P address in the said offences, which helps to trace the real accuse.

The Defense argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her. Further the Defense counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime proved beyond reasonable doubt. Additional Chief Metropolitan Magistrate, delivered the judgment on 5-11-04

This is the first conviction under the IT Act 2000 in India, the investigation is completed in minimum period means within seven month,

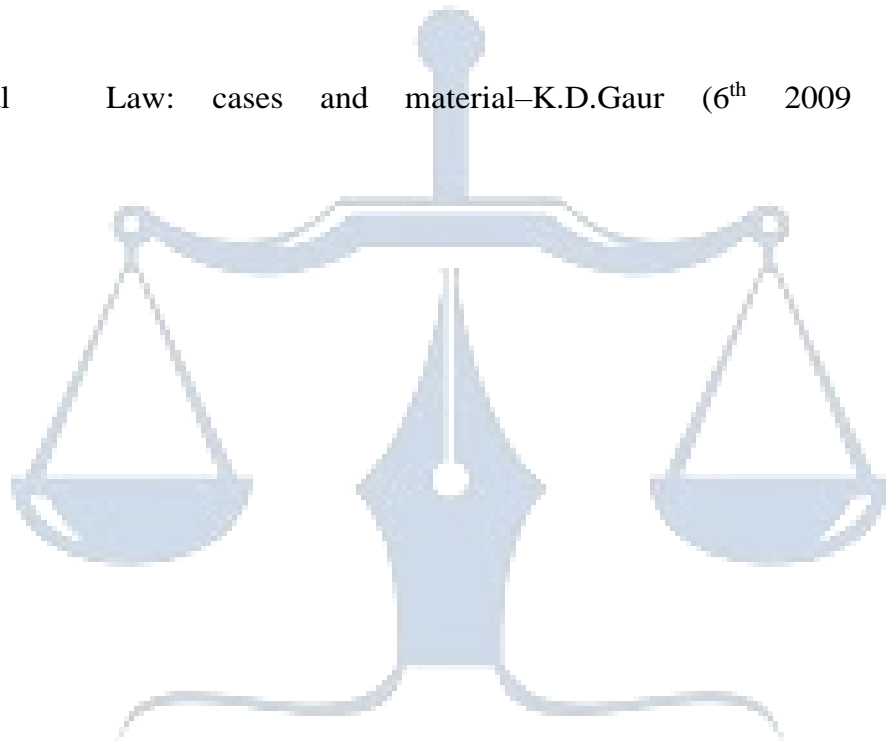
the judgment is pronounced by the Additional Chief Metropolitan Magistrate of Egmore, in the year 2004. The investigation and the trial completed in minimum period and the conviction given in the said matter.



WHITE BLACK  
LEGAL

## **BIBLIOGRAPHY**

1. Bharat's Supreme Court on Evidence Act. By A. S. Arora. Bharat Law House New Delhi, First Edition 2009.
2. Child in Cyber Space, by Ms Barkha B. Asia Law Book, Hyderabad. New edition 2008
3. Criminal Justices System – Dr. K.I Vibhutes ( Butterworth )
4. Criminal Law: cases and material–K.D.Gaur (6<sup>th</sup> 2009 Butterworth



WHITE BLACK  
LEGAL

Wadhwa, Nagpur)

5. Criminal Procedure Code – S.C. Sarkar (Indian Law House) New Delhi  
8<sup>th</sup> edi 2004
6. Criminal Trial and Investigations – Malik's Sultan, Prayag  
Publishing company, Allahabad , Edition 2013
7. Cyber law and crime – Barkha U Ram Mohan (Asia Law House)  
Hyd.
8. Cyber Crime and Legal Issues- Paul T. Augastine, Crescent  
Publishing Corporation , First publish in 2007
9. Cyber crime –Law and perspectives- Dr. Mrs.K.Sita Manikyam  
(Hind Law House)
10. Cyber Law & Cyber Crimes: Advocate, Prashant Mali Reprint  
Education 2013, Snow White
11. Cyber Law Cyber crime Internet And E-commerce: By  
Vimlendu Tayal, Bharat Law Publication, Jaipur, 2011
12. Cyber Law in India (Law on Internet) By Dr. Farooq Ahmed,  
New Era Law Publications Delhi, 2005, Pioneer Books.
13. Cybercrime; Talat Fatima, Eastern Book Company Lucknow.
14. E-Justices- Practical Guide for the Bench and Bar, By K.  
Pandurangan, Universal Law Publication, Edition 2009.
15. Forensic Science in Criminal investigation – Manoobhai G. Amin  
& Dr. Jai Shankar Singh, Unique Law Publishers, Jodhpur, Edition 2009
16. Forensic Science in Criminal Investigation and Trials By  
B.R.Sharma, Universal Law Publication, Fourth Edition, 2003.
17. Guide to Cyber Law – Rodney D. Ryder

18. Human Rights and Criminal Justices. By Pandit Kamalakar, Asia Law House, Hyderabad, First Edition, 2010



WHITE BLACK  
LEGAL

19. Judicial Jurisdiction in transnational cyber space - Bimal Raut.
20. Law relating to Electronic Contracts: By P.K. Singh, Lexis Nexis, Second Edition, 2016
21. Law of Crimes (Indian Penal Code, 1860) S.R.Myneni, Asia LawHouse, Hyderabad First edition 2009.
22. Malik's, Law relating to Criminal Trials. Law Publisher (India) Pvt. Ltd. 3<sup>rd</sup> Edition, 2004.
23. Police Diary – Mitter's , Law Publisher India, Allahabad, 11<sup>th</sup> Edition 2010
24. PSA Piliai's Criminal Law – Dr. K.I Vibhute (Tenth Edition 2008 Butterworth Wadhwa, Nagpur)
25. Social Dimension Of Law & Justices, Julius Stone, Universal Law Publishing Co. New Delhi, Edition (RP) 1999.
26. Textbook on, The Code of Criminal Procedure – By K. D.Gaur, Universal Law Publication, First Edition, 2016, Gurgaon, India.
27. The code of Criminal Procedure – Ratanlal & Dhirajlal, (Wadhwa, Nagpur)
28. The Indian Penal Code – Ratanlal & Dhirajlal (Wadhwa, Nagpur)
29. The Information Technology Act, 2000. By S. D. Dighe. Edition 2003, Hind Law House, Pune.
30. The Law of Evidence (As amended by Criminal Law (Amendment) Act, 2013 by M.P. Prasad and Manish Mohan, LexisNexis, Fifth Edition, 2013 Gurgaon, India.

**Webliography:**



1. [www.cyberlawindia.com](http://www.cyberlawindia.com)



WHITE BLACK  
LEGAL

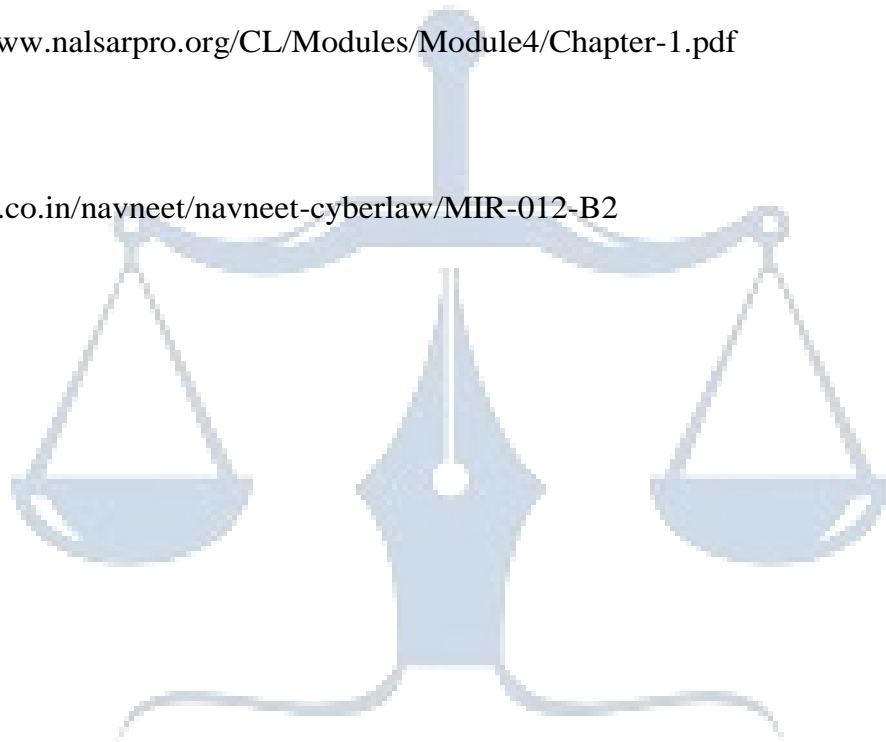
2. [www.indialaw.com](http://www.indialaw.com)
3. [www.cyberlawguide.com](http://www.cyberlawguide.com)
4. [www.supremecourtonline.com](http://www.supremecourtonline.com)
5. [www.caselaw.lp.findlaw.com/date/constitution/](http://www.caselaw.lp.findlaw.com/date/constitution/)
6. <http://shodhganga.inflibnet.ac.in/bitstream/10603/28181/9/09>
7. <http://www.legalindia.com/evolution-of-law-%E2%80%9Ca-short-history-of-indian-legal-theory%E2%80%9D/>
8. <http://www.shareyouressays.com/119646/essay-on-the-history-of-criminal-laws-in-india>
9. [https://en.wikipedia.org/wiki/Indian\\_Penal\\_Code](https://en.wikipedia.org/wiki/Indian_Penal_Code)
10. [www.legalservicesindia.com/.../the-elements-and-stages-of-a-crime-1228-1.html](http://www.legalservicesindia.com/.../the-elements-and-stages-of-a-crime-1228-1.html)
11. <http://www.articlesbase.com/criminal-articles/definition-of-crime-3317256.html>
12. [scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi](http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi)
13. [scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article](http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article)
14. [https://en.wikipedia.org/wiki/Recklessness\\_\(law\)](https://en.wikipedia.org/wiki/Recklessness_(law))

15. <http://hubpages.com/hub/Cyber-Crime>

16. <http://www.legalindia.com/cyber-crimes-and-the-law/>

17. <http://www.nalsarpro.org/CL/Modules/Module4/Chapter-1.pdf>

18. [tecindia.co.in/navneet/navneet-cyberlaw/MIR-012-B2](http://tecindia.co.in/navneet/navneet-cyberlaw/MIR-012-B2)



WHITE BLACK  
LEGAL

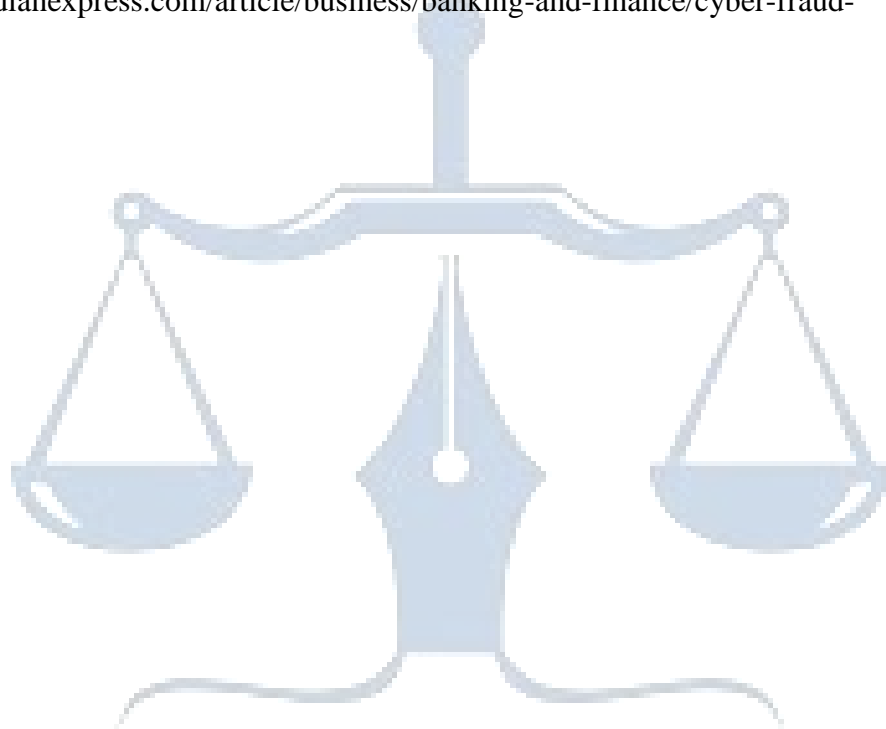
19. [http://www.naavi.org/pati/pati\\_cybercrimes\\_dec03.htm](http://www.naavi.org/pati/pati_cybercrimes_dec03.htm)
20. <https://en.oxforddictionaries.com/definition/cyberspace>
21. [http://catindia.gov.in/writereaddata/ev\\_rvnrbv111912012.pdf](http://catindia.gov.in/writereaddata/ev_rvnrbv111912012.pdf)
22. <http://www.lawteacher.net/administrative-law/essays/administration-of-criminal-justice-law-essays.php#ft>
23. <http://cyberforensicsofindia.blogspot.in/2013/03/regulations-and-guidelines-for.html>
24. <http://www.karnikaseth.com/evolving-strategies-for-the-enforcement-of-cyberlaws.html>
25. <http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/>
26. <http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/>
27. [http://cbi.nic.in/aboutus/manuals/Chapter\\_18.pdf](http://cbi.nic.in/aboutus/manuals/Chapter_18.pdf)
28. <http://www.mecs-press.org/>
29. <http://securelist.com/analysis/publications/36253/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/>
30. <http://www.techrepublic.com/blog/data-center/uk-cyber-crime-laws-updated/>
31. <http://www.minterellison.com/publications/cybercrime-privacy-update-201305>

32. <http://www.businessdictionary.com/definition/cyberspace.html#ixzz42Nri8Cg> F

33. <http://en.wikipedia.org>.

34. <http://www.Indianweb2.com>.

35. <http://indianexpress.com/article/business/banking-and-finance/cyber-fraud-> bank-



WHITE BLACK  
LEGAL

atm-debit-cards-sbi-rbi-online-banking-security-3094094/

36. <http://www.cyber.law.harvard.edu/media/files/wpsupplement2005.pdf>
  
37. <http://www.cyberlawconsulting.com/cyber-cases.html>
  
38. <http://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/>
39. <http://www.oneindia.com/feature/conviction-rate-cyber-crime-is-0-5-per-cent-here-are-the-reasons-1609728.html>
40. <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>

