A STUDY ON CYBER CRIME AND IT'S INVESTIGATION WITH SPECIAL REFERENCE TO PUNE DISTRICT

A SYNOPSIS SUBMITTED

TO

SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY, NANDED

For the award of degree of

DOCTOR OF PHILOSOPHY

In Law Under the faculty of Law

Under the guidance of

DR. R. B. DHESHMUKH,

RESEARCH CENTRE

SHIVAJI LAW COLLEGE, PARBHANI

By

MS. AAMRAPALI VIJAYKUMAR KASTURE

B.SL., LLB., LLM.

RESEARCH PROPOSAL

A STUDY ON CYBER CRIME AND IT'S INVESTIGATION WITH SPECIAL REFERENCE TO PUNE DISTRICT.

INTRODUCTION

Crime being a social phenomenon can find its existence since the period of existence of human civilization. As it is a human tendency to certain extent it exist in one way or the other in every era of human civilization. As the nature of social structure changes from one form to another the nature of the offence / crime also get changed accordingly. In ancient days the nature of offence/ crime was basically against the human body, Property, Status etc and was directly related to the same. Now we are entering into 21st Century and this era is an era of computerization/ digitalization etc and accordingly the nature of transaction/s, communication/s and safety etc are maximum based on such digitalization. Even the Government Policy is also of such nature that, the maximum business/ commercial transactions should be done in the same manner. It ultimately going to open the doors for the offences of new nature. ie. Cyber Crime.

Considering the changing nature of social structure our systems also need to get well equipped to cope up the new challenges in the area of investigation and trail of cyber crime. We wish to study the same subject in and around Pune region as Pune is one of the most emerging Metro cities in India having huge Information Technology based Companies in India and as a city ideally representing the rest of the cities in India.

STATEMENT OF PROBLEM

The human civilisation is a continuous process of social changes over a period of time. it includes the changes not only in social aspect but it also includes the economical as well. Most of the time these changes are nothing but an outcome of technological developments in the society and such a changes resulted in modernization in the society as well. An invention of computer initially was only for the purpose of mathematical calculations just to ease and to expedite the process of complicated calculations but gradually the use of computer is started occupying

almost every single aspect of day to day life. The use of computer with the help of internet has brought a very drastic change in the society and the whole world come together like a family. The effect of rapid globalization and the requirement of urban development, it is a need of time that commercial activities have to be gets done by privatization. The collective effect of the rapidly growing liberalization, globalization and privatization is nothing but the outcome of digitalization and use of internet by the world. It ultimately causes the rapid growth in crime related to the cyber world.

The increased use of the cyber world by the masses across the world is again a matter of concern as majority of the people using the internet facility are not at all aware about the proper logical and ethical use of the cyber world which ultimately resulted into the rapid growth in cyber crime.

SIGNIFICANCE AND UTILITY OF THE RESEARCH

One of the most significant and influential inventions of 20th century was the Computer. There has been a sea change in the purposes and the manner in which computers are used with advent of microprocessor technology and digital communication. The computer started with being a giant calculating machine. It then metamorphosed itself into a standalone personal tool for performing assorted routine tasks like word processing and accounting and then to todayós network device permeating virtually everything including instantaneous and global personal and business interaction. The way business is conducted and records are maintained today is a far cry from days past. Accordingly, in enforcement agencies including the Income tax department, more and more information is being stored, transmitted or processed in digital form.

Though at once it looks very significant and most useful medium of communication and business activities in modern days, it also carries certain very definite but unseen before threat and concern along with it. The threat of cyber crime in almost every sector the this modern days invention is getting used and to cope up with the unseen and un-estimated risk of cyber crime we need to have thorough study of the subject with all the dimensions since the causes of cyber crime to the actual trail of the cyber crime cases along with the study of corrective measures to prevent the cyber crime.

Apparently it is understood that, the number of the unintentional acts resulted into the Cyber crime is only because of serious lacks of awareness about the proper and ethical use of the electronic gazette and this research would be an attempt to bring social awareness about the proper and ethical use of advance technology based electronic gazettes with an intent to prevent cyber crimes in the society. The research would definatly would be helpful to suggest corrective measures in order to prevent the occurrence of Cyber Crime in the society.

The research will be helpful to find out the loop wholes and lacuna in the modus operandy in the existing investigation process as well as to strengthen the good and effective parts in the process of the analysis and scrutiny of the collected digital evidence by way of investigation of the Cyber Crime to help the judiciary to conduct effective trail of cyber crime

The research would surely be very handy and helpful to the intellectuals, Corporate executives, academics, people working in and for various Government and para Government Departments like Income and other Tax Department/s, Revenue Departments, Defense and Home Department, Foreign exchange and allied departments, various investigation agencies like Police Department, CBI, CID, SID, ATS, EOW etc in use of their day to day activities while using electronic gazettes in the discharge of their official duties.

AIMS AND OBJECTIVES OF THE RESEARCH

1) TO STUDY THE ROOT CAUSE OF THE CYBER CRIME

2) TO IMPROVE THE INVESTIGATION OF CYBER CRIMES

3) TO IMPROVE THE TRAIL OF THE CASES RELATED TO CYBER CRIME IN PUNE DISTRICT

4) TO SUGGEST CORRECTIVE MEASURES TO PREVENT CYBER CRIMES

5) TO BRING SOCIAL AND LEGAL AWRENESS IN SOCIETY ABOUT THE CYBER CRIMES

HYPOTHESIS

1. lack of knowledge amongst the society about the cyber crimes,

2. Present investigation machinery demands improvements in the area of cyber crime investigation

3. A need of an hour about the awareness regarding the cyber crimes and related issues.

RESEARCH METHODOLOGY

DOCTRINAL AND NON DOCTRINAL:-

DOCTRINAL:- The Doctrinal research means a research which is carried out upon the legal propositions or propositions by way of analysing the existing statutory provisions and cases by applying the reasoning statutory provisions and the cases by applying reasoning power.

In other words it means and includes the analysis of legal institutions through legal reasoning and rational deduction.

EMPIRICAL OR NON DOCTRINAL:- It basically means a study or research carried out by collecting and gathering data or information by a firsthand study. in other words it means relaying solely upon observations and experiment and not on theories. It also called as Fact research.

To understand the scope of the Empirical or Non Doctrinal research it is said that," By fact research in law, it means a systematic search into social, political and the other fact conditions which give rise to individual rules and examination of the social, political and other effects of these rules.

Considering the nature and scope of the study of the present subject, it clearly requires the actual filed work such as collection of information and data from various

Governments Departments, Investigation Agencies, Judiciary and other concerned related offices even by taking interview of the concerned officer/s.

It also may involve the analysis of the legal propositions and all the relevant legal provisions so the research methodology may be used for the present study involve both Doctrinal as well as Non Doctrinal or Empirical research.

As it may include field work for legally possible data collection from the Police Departments/ Court of Law/ Cyber Cell etc the research methodology would be Non doctrinal.

AREA OF RESEARCH

The research in hand is essentially based upon the cyber crime, its investigation and trail in Pune district and as such the area of the research would be to study the causes of cyber crime in various fields like offences under IPC, IT Act and offences relating to various kinds of business activities. As the research also includes the investigation of the cyber crime area of the study also includes the various investigation agencies and their modus operandy. The research in hand also includes to study the actual trail of cyber crimes with intent to analyze the process of trail to improve the same by suggesting the corrective measures by removing the lacunas in the same.

REVIEW OF LITERATURE

The law of the country has also taken cognizance of this reality. The Information Technology Act, 2000 has been enacted recognizing electronic records as evidence, governing access to and acquisition of digital and electronic evidence from individuals, corporate bodies and/ or from the public domain. By way of this enactment, amendments were also brought in other laws like Indian Penal Code, Indian Evidence Act and Criminal Procedure Code, (Cr.PC). The Income-tax Act, 1961 has also been amended thrice by way of Finance Act 2001, Finance Act 2002 and Finance Act 2009 thereby according recognition to electronic evidence, facilitating access to them and giving when need be, powers to impound and seize them. By Finance Act, 2001, Clause (22AA) was inserted in Section 2 to provide that the term "document" in Income Tax Act, 1961, includes an electronic record as

defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000. By Finance Act, 2002, Clause (iib) was inserted in Sub-Section (1) of Section 132 requiring any person who is found to be in possession or control of any books of account or other documents maintained in the form of electronic record as defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000), to afford the authorised officer the necessary facility to inspect such books of account or other documents; and by Finance Act, 2009, clause (c) was inserted in sub-section (1) of Section 282 providing that service of notice in the form of any electronic record as provided in Chapter IV of the Information Technology Act, 2000 (21 of 2000) will constitute valid service.

SCHEME OF PRESENTATION

Research work on the topic has been presented in the form of thesis by dividing it into the following 7 chapters.

CHAPTER I : INTRODUCTION

It contents an introduction to the concept of A STUDY ON CYBER CRIME AND IT'S INVESTIGATION WITH SPECIAL REFERENCE TO PUNE DISTRICT, The Area of Research, The Significance of The Topic of the Research, Aims and Objects of the Research, Hypothesis, Review of Literature, The Methodology followed for the Research and the Scheme of Presentation of the Research work**.**

It today's environments, most businesses and government processes could not survive without the computer-especially email or totally web-based businesses. Without computers, entire businesses and government operations would almost cease to function. Criminals use computers to support their illegal operations. Computer crimes and frauds are increasing day by day in the changing social circumstances. They will no doubt continue to increase as more computers are networked internationally, thus giving global access to computer criminals.

Cyber space has no specific jurisdiction; therefore, criminals can commit crime from any location through computer in the world leaving no evidence to control. Protection of information is keeping symbolic representation from harm or in other words it is preventing harm caused by symbolic representations. It is a form of self-defense in cyberspace which cannot be left to others. It is very difficult to control cyber crime because (i) criminals are well aware about security and preventive measures; (ii) they hardly leave any evidence; (iii) lack of adequate legislation to control them; (iv) lack of awareness among users; (v) lack of defined jurisdiction in cyberspace, cybercrimes took international shape; (vi) traditional laws are not adequate and present information technology law is not enough to prevent and control cyber crimes; (vii) cyber crimes are not adequately defined and scope is not specified; (viii) lack of expert law enforcing agencies with infrastructural support; and (ix) lack of expert judicial system with infrastructure.

Cyber crime is a threat to national and international socio-economic, political and security system. The increasing use of the Internet has also led to an increase in cyber crime. When internet was developed, its founding fathers did not probably imagine that internet could also be misused for criminal activities. However, today there are many disturbing things happening in cyber space, especially the cyber crimes. It will not be out of place to mention here that cyber crime has acquired international dimensions and that today the cyber criminals can move at the speed of light on a highway on which there are no traffic signals, no constables and no custom or immigration authorities to check them for anything.

Traditionally the duration of criminal acts in measured in minutes, hours, days, weeks, months and years. Thus automated crime must be considered in terms of a computer time scale of milliseconds, microseconds and nanoseconds because of the speed of execution of instructions in computers. Computer crime may involve computers not only actively but also passively. If a computer is stolen in a simple theft where, based on all circumstances, it could have been a washing machine or milling machine, knowledge of computer technology is not necessary and it would not be a computer crime. However, if knowledge of computer technology is necessary to determine the value of the article taken, the nature of possible damage done in the taking or the intended use by the thief, then the thief would be a computer crime.'

Cyber crimes are not any new crimes. They are just the traditional crimes committed through computer and internet.

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and various services.

The term 'cyber' means ña prefix overused to indicate a connection to computers, networks, technology or futurism.ò 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 is defined as ña legal wrong that can be followed by criminal proceedings which may result into punishment." A crime may be said to by any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber crime is a broad and generic term that refers to crimes committed using computers and the internet. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. In other words computer crimes are those that are committed either on a computer system or with the aid of such a system.

The IT Encyclopedia .com define the word ócyber crimeô as ñcriminal activities in cyber spaceò. Cyber crime has been defined as the act of creating, distributing, altering, stealing, misusing and destroying information thorough the computer manipulation of cyberspace; without the use of physical force and against the will or the interests of the victim. As a concept, information can be anything from electronic money, to government secrets, and the victim can be an individual, a corporate person, or as criminal law is defined the state and society as a whole.

óCyber crimeô or óComputer Crimeô generally speaking computer crime is a form of white-collar crime, meaning thereby, that it is usually committed by the individuals/ professionals or organizations during the course of their occupation/profession etc. Nevertheless, some of the commonly spelt out definitions of ócyber crimeô are:

A criminal activity that involves unlawful access to, or utilization of, computer systems.

- Any illegal action in which a computer is used as a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the functions of a computer.

- Any incident 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.

- Any violation of the law in which a computer is the target of or the mean for committing crime.

The Organization for Economic and Cultural Development (OECD) however, has adopted the following definition as the working definition for computer-related crime or computer crime ñcomputer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of dataò. Cyber crime means any activity which involves the unauthorized and unlawful access to or utilization of computer system or networks in order to tamper with the data or to intentionally transact anything illegal with the help of computers and the Internet can broadly be called as ócyber crimeô.

Cyber crime means ñwhen a computer is used in the commission of such crime or computer technology is responsible for the wrongful gain or wrongful loss of a party or there has been an illegal use of computers in the processing and transmission of data.

To conclude, it may be stated that various terms and definitions that came into scene have only helped in obfuscating the concept further. What exactly is a computer crime or cybercrime? We can safely state that these terms are not amenable to a precise definition.1 It could simply be a technological rendition of a traditional crime or it could be an innovative crime that came up due to prevalence of computers and networks. That is why mt6ost of the world legislations fighting cybercrime do not attempt a definition of the term.

Cyber crimes-harmful acts committed from or against a computer or network-differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

CUASES OF CYBER CRIME

The basic reasons behind the occurrence of cyber crime is massive unawareness / Ignorance about the proper and ethical use of the most beautiful facility like cyber world and all other traditional causes of crime as social phenomenon.

DEVICES THAT CAN BE USED / INVOLVED IN THE CYBER CRIME

The use of digital devices in day to day life has increased tremendously. To help the understanding of the investigating officers, a compilation of various devices and the potential evidences these devices may contain is provided below;

1) A Desktop Computer,

2) Pen Drives,

3) Hard Drives,

4) Handheld Devices, like Mobile Phones, (Smart Phones), Electronic Organizer, IPAD, Personal Digital Assistant etc

5) Smart cards, Dongles and Biometric Scanners

6) Display Monitor (CRT/LCD/TFTetc), Screens of Mobile Phones if switched on

7) Answering Machines

8) Local Area Networks (LAN) Card or Network Interface Cards

9) Modems, Routers, Hubs and Switches

10) Servers

11) Removable storage devices like SD Cards in Mobile phones

12) Scanners and Copiers

13) Digital Cameras

14) Pagers

15) CD/DVDs/

16) Facsimile Machines

17) Global Positioning Systems(GPS)

18) Cloud Data Servers

CHAPTER II:- CONCEPTUAL STUDY OF CYBER CRIME

1) CONCEPT OF CYBER CRIME AND ITS INVESTIGATION.

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and various services. The term 'cyber' means ña prefix overused to indicate a connection to computers, networks, technology or futurism.ò 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 is defined as ña legal wrong that can be followed by criminal proceedings which may result into punishment." A crime may be said to by any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber crime is a broad and generic term that refers to crimes committed using computers and the internet. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks

are used to enable the illicit activity. In other words computer crimes are those that are committed either on a computer system or with the aid of such a system.

The IT Encyclopedia.com defines the word ócyber crimeô as ñcriminal activities in cyber spaceò. Cyber crime has been defined as the act of creating, distributing, altering, stealing, misusing and destroying information thorough the computer manipulation of cyberspace; without the use of physical force and against the will or the interests of the victim. As a concept, information can be anything from electronic money, to government secrets, and the victim can be an individual, a corporate person, or as criminal law is defined the state and society as a whole.

óCyber crimeô or óComputer Crimeô generally speaking computer crime is a form of white-collar crime, meaning thereby, that it is usually committed by the individuals/ professionals or organizations during the course of their occupation/profession etc. Nevertheless, some of the commonly spelt out definitions of ócyber crimeô are:

2) HISTORY OF CYBER CRIME:-

Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others sought to gain sensitive, classified material. Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers.

3. CLASSIFICATION OF CYBER CRIME.

4. SPECIAL SKILLED INVESTIGATION OFFICER, PUBLIC PROSECUTER / JUDGES / COURT.

5. MEASURES TO PREVENT CYBER CRIME:-

A. BY MAKING SUITABLE CHANGES, AMENDMENTS IN PRESENT LEGAL PROVISIONS,

B SOCIAL AWARNESS ETC.

CHAPTER III :- CONSITUTIONAL AND LEGAL PROVISIONS REGARDING CYBER CRIME AND ITS INVESTIGATION

RELEVANT LEGAL PROVISIONS FORM IT ACT AND IPC ETC.

The Legal Background:

The Information Technology Act-2000 has been enacted to provide legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, which involve the use of alternatives to paper-based methods of communication and storage of information. The same enactment has also brought amendments in the **Indian Penal Code, 1861**, the **Indian Evidence Act, 1872**, the **Bankers' Books Evidence Act**, **1891** and the **Reserve Bank of India Act, 1934**.

Under Indian **Evidence Ac**t there are several references to documents and records and entries in books of account and their recognition as evidence. By way of THE SECOND SCHEDULE to the Information Technology Act Amendments to the Indian Evidence Act have been brought in so as to, incorporate reference to Electronic Records along with the document giving recognition to the electronic records as evidence.

Further, special provisions as to evidence relating to electronic record have been Inserted in the Indian Evidence Act, 1872 in the form of section 65A & 65B, after section 65. These provisions are very important. **They govern the integrity of the electronic record as evidence, as well as, the process for creating electronic record. Importantly, they impart faithful output of computer the same evidentiary value as original without further proof or production of original.** Accordingly, while handling any digital evidence, the procedure has to be in consonance of these provisions.

Under **Indian Penal Code** several acts of omission and commission relating to various documents and records are treated as offences. By way of THE FIRST SCHEDULE to the Information Technology Act, Amendments to the Indian Penal Code have been brought in, so as to incorporate reference to Electronic Records along with the document.

As far as **Income-tax Act, 1961** is concerned; it has been amended thrice by way of **Finance Act, 2001, Finance Act, 2002 and Finance Act, 2009** respectively.

By way of first amendment, provisions of sub-section (12A) of section 2 was inserted to give legal recognition to the books of account maintained on computer and sub-section (22A) to section 2 was inserted to provide definition of documentö which included electronic record as defined under Information Technology Act 2000. Under Information Technology Act 2000 an electronic record has been defined to include data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro file. This definition of electronic record is wide enough to cover person in possession of computer, storage device, server, mobile phone, i-Pod or any such device. The above amendment has thus specifically given recognition to electronic record as admissible evidence at par with a documentö. Further, the powers to impound/copy a document during a survey action u/s 133A and power to seize a document during a search and seizure operation has also been automatically extended to electronic records as a result of the amendment.

By way of second amendment, provisions of section 132 (1) (iib) were inserted facilitating access to the electronic devices including computer, containing document or books of accounts in the form of electronic records by making 18 it obligatory for the person under control of such device to afford the necessary facility to inspect such records.

By Finance Act, 2009, clause (c) was inserted in sub-section (1) of Section 282 providing that service of notice in the form of any electronic record as provided in Chapter IV of the Information Technology Act, 2000 (21 of 2000) will constitute valid service.

The various provisions of the Constitution of India provides various fundamental rights to the every citizen of India, more particularly in PART III under the head of FUNDAMENTAL RIGHTS containing Articles 12 to 35 deals with the same. It also deals with the rights to constitutional remedies under Article 32 and 226 respectively. All these provisions now has a added dimension to the basic concept of the fundamental rights of an individual in the rapidly changing social structure.

CHAPTER IV:- INFORMATION TECHNOLOGY ACT AND ITS PROVISIONS:-

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

CHAPTER V:- STATASTICAL DATA AND ITS ANALYSIS.

All the statistical data would be collected and gathered during the course of study hence all the statistical data would be provided while concluding the study **then analysis of the said data.**

CHAPTER VI JUDICIAL TRENDS RELATED TO CYBER CRIMES:-

Different cases regarding Cyber Crime in India and Abroad.

HACKING,

Sanjay Kumar Vs. State of Haryana [CRR No. 66/2013 (O and M)]

Just Dail Vs. Infomedia 18 Delhi HC.

DATA THEFT

T - Mobile data Theft case. Chester Crown Court, June 2011.

CYBER FISHING

State of Maharashtra Vs. Opera Chilezein Josoph and Others (C.R. No. 344/2012)

Sri Umashankar Sivasumbramaniam Vs. ICICI Bank (Peti. No. 2462 / 2008)

CYBER STALKING

Manish Kathuria case New Delhi 2001. (First case of arrest in India for syber stalking U/s. 509.)

E-mail SPOOFING

State of Maharashtra Vs. Pranab Mitra 2011.

CREDIT CARD AND ONLINE BANKING FRAUD.

Sanjay Dhande Vs. ICICI Bank and Vodafone Jan 2014.

Delhi Credit Card Fraud Case

COPY RIGHTS IN INTERNET ERA.

Hindustan Times Vs. www.legalpandits.com 2001 Delji HC.

PORNOGRAPHY

State Vs. T.S. Balan & Aneesh Balan, Kerla. (Morphing Priest and his Son got first conviction in committing a cyber crime**)**

CHILD PORNOGRAPHY

Hariram Vs. State of Rajastan Cr. appeal No. 907 /2009 arising out of SLP (Cr.) 3336/2006.

ONLINE GAMBELING

case of Cyber Lotto of Kola Mohan**.**

ONLINE SELLING

Sanjay Kumar Kedia Vs. Narcotics Control Bureau 2007 SC.

CYBER DEFAMATION IN INDIA

Tata Sons Vs. Greenpeace International Delhi. HC IA 9089/2010 in CS (OS)1407/2010.

SMC Pneumatics India Pvt. Ltd. Vs. Jogesh Kwatra

Avnish Bajaj Vs. State (2005) 3 Copm LJ 364 Del.

Vyakti Vikas Kendra, India Public Charitable Trust through Trusty Vs. Jitendra Bagga CS (OS) No. 1340/2012. Delhi HC 2012

Google India Pvt. Ltd. Vs. Visaka Industries Limited CP No. 7207 of 2009.

UNITED NATIONS

Stannley Young Vs. New Haven Advocate 184 F. Supp. 2d 498 (2001)

Katherine Griffis Vs. Morianne Luban C3-01-296

Zeran Vs. America Online Inc. 12 F 3d 327 (4th Cir 1997)

stratton Oakmount Vs. Prodigy Services Co. 1995 WL 805178 (NY Sup.)

Blumenthal Vs. Drudge and American Online Inc. 992. F. Supp.44 1998

SOFTWARE PIRACY

Microsoft Corporation Vs. Yogesh Papat, Delhi HC.

PERSONAL SENSITIVE INFORMATION.

Rohit Maheshwari Vs. Vodafone 2013.

CHAPTER VII:- CONCLUSION, FINDING AND SUGGESTIONS.

Depends upon the completion of the study.

BIBLOGRAPHY

- **Gaur, K.D. (2006). The Indian Penal Code, Third Edition, Universal Law Publishing Company Pvt. Ltd.**
- **Ahmad Farooq, Cyber Law in India, Pioneer Books, New Delhi.**
- **Joga Rao, S.V. (2004). Law of Cyber Crimes and Information Technology, Wadhwa & Co. Nagpur.**
- **Digital Evidence Investigation Manual by Income Tax Department.**
- **Information Technology Act 2000 (21 of 2000) along with**

  a) The Digital Signature (End Entity) Rules, 2015

  b) The Cyber Appealate Tribunal (Power and Functions of the Chairperson) Rules 2016.

  c) The Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules 2016.

  Published by PROFESSIONAL BOOK PUBLISHERS.

- **Code of Criminal Procedure 1973 Eleventh Edition by SC Sarkar and PC Sarkar published by LexisNexis**
- **Direct Taxes Law and Practice Publisher Taxman's with special reference to Tax planning, Author – Dr. Vinod K. Singhania & Dr. Kapil Singhania, 58th Edition, 2017-18.**
- **Indian Penal Code, 1861, (AS AMENDED FROM TIME TO TIME) Published by Indian Law House.**
- **Indian Evidence Act, 1872, (AS AMENDED FROM TIME TO TIME) 19th edition BY Sir John Woodroffe and Syed Amir Ali revised by B. M. Prasad and Manish Mohan published by LexisNexis Butterworths Wadhwa.**
- **Seth's Commentary on Bankers' Books Evidence Act, 1891 (AS AMENDED FROM TIME TO TIME) 3rd Editions Published by Law Publishers (India) Pvt. Ltd.**

- **Reserve Bank of India Act, 1934 (AS AMENDED FROM TIME TO TIME) 25th Edition by ML Tannan revised by NV Srinivasan by LexisNexis**
- **Journals and Periodicals,**

  a) AIR from 2001 to update.,

  b) Cri. L. J. from 2001 to update

- **NEWS PAPERS etc.**

WEBLOGRAPHY

- **site http://shodhganga.inflibnet.ac.in/**
- **http://www.srtmun.ac.in/en/**

TABLE OF CASES

Sr.No.	**Details of Case**
1.	**HACKING** • Sanjay Kumar Vs. State of Haryana [CRR No. 66/2013 (O and M)] • Just Dail Vs. Infomedia 18 Delhi HC.
2.	**DATA THEFT** • T - Mobile data Theft case. Chester Crown Court, June 2011.
3.	**CYBER FISHING** • State of Maharashtra Vs. Opera Chilezein Josoph and Others (C.R. No. 344/2012) • Sri Umashankar Sivasumbramaniam Vs. ICICI Bank (Peti. No. 2462 / 2008)
4.	**CYBER STALKING** • Manish Kathuria case New Delhi 2001. (First case of arrest in India for cyber stalking U/s. 509.)
5.	**E-mail SPOOFING** • State of Maharashtra Vs. Pranab Mitra 2011.
6.	**CREDIT CARD AND ONLINE BANKING FRAUD.** • Sanjay Dhande Vs. ICICI Bank and Vodafone Jan 2014. • Delhi Credit Card Fraud Case

7.	**COPY RIGHTS IN INTERNET ERA.** • Hindustan Times Vs. www.legalpandits.com 2001 Delji HC.
8.	**PORNOGRAPHY** • State Vs. T.S. Balan & Aneesh Balan, Kerla. (Morphing Priest and his Son got first conviction in committing a cyber crime**)**
9.	**CHILD PORNOGRAPHY** • Hariram Vs. State of Rajastan Cr. appeal No. 907 /2009 arising out of SLP (Cr.) 3336/2006.
10.	**ONLINE GAMBELING** • Case of Cyber Lotto of Kola Mohan**.**
11.	**ONLINE SELLING** • Sanjay Kumar Kedia Vs. Narcotics Control Bureau 2007 SC.
12.	**CYBER DEFAMATION** • Tata Sons Vs. Greenpeace International Delhi. HC IA 9089/2010 in CS (OS)1407/2010
13.	**SOFTWARE PIRACY** • Microsoft Corporation Vs. Yogesh Papat, Delhi HC.
14.	**PERSONAL SENSITIVE INFORMATION.** • Rohit Maheshwari Vs. Vodafone 2013.

Submitted by

MS. AAMRAPALI VIJAYKUMAR KASTURE,

B.SL., LL.B.,LL.M., D.C.L.

D - WISTERIA PARK, 804 -A, WADGAO

FLYOVER, BOMBAY - PUNE HIGHWAY,

WADGAO BK.TALUKA HAVELI, PUNE 41.

Mob. No. 9823132324