CYBER CRIME AND LAWS IN INDIA

A DISSERTATION

SUBMITTED TO NATIONAL LAW SCHOOL OF INDIA UNIVERSITY IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF

MASTERS IN LAW

BY
KULDEEP BAIRWA
(ID: 887/2019)

Under the Guidance and Supervision of

Dr. A. Nagarathna
Associate Professor of law

CANDIDIATE DECLARATION

I hereby certify that the work which is being presented in the dissertation entitles **"CYBER CRIME AND LAWS IN INDIA"** in partial fulfilment of the requirements for the award of the Degree of Masters in Law and submitted to the National Law School of India University, Bangalore is an authentic record of my own work and carried out during a period of November 2019 to May 2020 under the supervision of Dr. A. Nagarathna, Associate Professor of law. The matter presented in the thesis has not been submitted by me for the award of any degree of this or any other Institute.

Date (Kuldeep Bairwa)

Place: Bangalore Id- 887/2019

CERTIFICATE

This is to certify that the research work being reported in the dissertation entitled **"CYBER CRIME AND LAWS IN INDIA"** is the original contribution of the candidate and the work has not been presented anywhere else for the award of any other degree to the best of my knowledge.

(Dr. A. Nagarathna,)

Associate Professor of law

National Law School of India University

Bangalore.

ACKNOWLEDGEMENT

The acknowledgment of this milestone would be incomplete without expressing my heartfelt gratitude to my dissertation guide **Dr. A. Nagarathna** (Associate Professor of Law) for his invaluable guidance and support through the course of the dissertation. I wish to thank him for permitting me to pursue my area of interest as the core theme of my research work and thereafter guiding me in all aspects of my researching. His continuous motivation and support were Driving factors in completing my research.

I also sincerely thank our Vice-Chancellor, **Prof. (Dr.) Sudhir Krishnaswamy** whose constant encouragement, ardour and dedication towards the LL.M. batch 2019-2020 were an immense source of inspiration with regard to completing the dissertation. I also thank my other faculty members, library staff members and my friends for helping me in every capacity possible towards the successful completion of my dissertation.

Lastly, I wish to thank my parents, brothers and my friend Aratrika Das and Almighty for believing in my capabilities and being strong pillars of support throughout the course of my dissertation.

TABLE OF CONTENT

Particulars	Page No.
Candidate's Declaration	ii
Certificate	iii
Acknowledgement	iv
Table of content	v-ix
List of Abbreviation	x
List of Cases	xii
Chapter I Introduction	1-5
• Introduction	1
• Statement of problem	1
• Objective of the study	2
• Scope and limitation	2
• Hypothesis	2
• Research question	3
• Research methodology	3
• Literature review	3
• Tentative Chapterization	5

Chapter II concept of the cybercrime and types of the cyber crime	6-27
• Concept of cyber space	7
• Modern concept of crime	8
• Nature of Crimes	8
• Fundamental Elements of Crime	10
• Criminal Liability under Cyber Crimes	13
• Meaning and concept of the cyber crime	14
• Definition of Cyber crimes	14
• Traditional Crime and Cyber Crime	15
• Relation between Cyber Crime and Cyber Security	16
• Elements of cyber security	18
Types of cyber crime	21
• Cybercrime against the person	21
• Cyber crime against the property	22
• Cyber crime against government	23
• Cyber crime against society	24
• Cyber crime during Covid-19	25

Chapter IV Anaysis of Information Technology Act 2000	28-41
• Application	28
• Definition	28
• Digital signature	29
• Penalties	30
• adjudication	32
• Offences	33
• Due diligence	38
• Observation on ITA and ITAA	39
Chapter IV Cases related to the cyber crime in India	42-55
• Bois Locker Room case	42
• Pune Citibank MphasiS Call Center Fraud	45
• sony.sambandh.com case	46
• The Bank NSP Case	47
• SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra	47
• Tamil Nadu Vs Suhas Katti AIR 2004	48
• Cosmos Bank Cyber-Attack in Pune	48
• Hack Attack on Indian Healthcare Websites	49
• Shreya Singhal v Union of India	49

• Ritu Kohali Case	50
• Sanjay Kumar v. State of Haryana	51
• Lakshmana Kailash K.case	51
• Yahoo Inc. v Akash Arora & Anr	52
• Mr. Arun Jaitley vs Network Solutions Private ltd	53
• Sandeep Varghese Vs. State of Kerala	53
• Syed Asifuddin & other v. The State of Andhra Pradesh & Another	54
• Abhinav Gupta v. State of Haryana	54
• National Association of Software v. Ajay Sood & Other	55
• Shri Umashankar Sivasubramaniam v. ICICI Bank	55
Chapter V Analysis of Information Technology laws of UK and US	56-60
IT Laws of UK	56
• Cybersecurity and the uk legal landscape	56
• Computer misuse act, 1990	56
• Computer misuse act amendments	58
• Problems	58
• Spam, malware and the law	59
• The police and justice act 2006	61

• European convention on cybercrime	61
• Personal internet security	62
• Crime and punishment	62
• Using civil law to deal with cybercriminals	63
• Balancing security and freedom	63
IT Laws of US	64
• Consumer privacy protection act 2017	65
• Computer fraud and abuse act [cfaa]	65
• Electronics communication privacy act [ecpa]	67
• Federal laws	68
• Federal cybersecurity laws	68
Chapter VI Conclusion and Suggestions	70-73
Table of statute	74
Bibliography	75-77

LIST OF ABBREVIATIONS

&	And
%	Percent
AD&SJ	Additional District and Session Judge
CFAA	Computer Fraud and Abuse Act
CISA	Cyber security Information Sharing Act
CPC	Code of Civil Procedure
Cr.PC	Code of Criminal Procedure
DCP	Deputy Commissioner of Police
DGP	Director General of Police
DoT	Department of Telecommunication
DSP	Deputy Superintendent of Police
ECPA	Electronics Communication Privacy Act
FIR	First Investigation Report
GOI	Government of India
HC	High Court
IDRBT	Institute for Development of Research in Banking Technology
IPC	Indian Penal Code
ISP	Internet Service Provider
IT	Information Technology

ITAA	Information Technology Amendment Act
MNC	Multi National Company
NHTCU	National Hi-Tech Crime Unit
PO	Police Officer
POCSO	Protection of Chil Dren from Sexual Offences
SC	Supreme Court
SCA	Stored Communications Act
Sec.	Section
SOCA	Serious Organised Crime Agency
SWIFT	Society for Worldwide Interbank Telecommunications
UNCITRAL	The United Nations Commission on International Trade Law
UNGA	United Nation General Assembly
WWW	Worldwide Web

TABLE OF CASES

- Abhinav Gupta v. State of Haryana
- Bazee.com case
- Bhim Sen Garg v. State of Rajasthan and Ors
- Bois Locker Room case
- Cosmos Bank Cyber-Attack in Pune
- DPP v. Bignell
- Lakshmana Kailash K.case
- Mr. Arun Jaitley vs Network Solutions Private ltd
- National Association of Software v. Ajay Sood & Other
- Pune Citibank MphasiS Call Center Fraud
- R v. Bedworth
- Ritu Kohali Case
- Sandeep Vaghese v/s State of Kerala
- Sanjay Kumar v. State of Haryana
- Sharat Babu Digumatri v. Government of NCT Delhi
- Shreya Singhal v Union of India, AIR 2015 SC 1523
- Shri Umashankar Sivasubramaniam v. ICICI Bank
- SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra
- sony.sambandh.com case
- Syed Asifuddin & other v. The State of Andhra Pradesh & Another
- Tamil Nadu Vs Suhas Katti AIR 2004
- The Bank NSP Case
- Yahoo Inc. v Akash Arora & Anr.

CHAPTER I

INTRODUCTION

Introduction

The world is facing a great malady called cybercrime since the last two decades. Use of the malevolent programs in computers and over internet by malicious people to attack data or sell contraband and someone else's identity is known as cybercrime. This type of crime is committed with the use of computers and internet. A cybercrime criminal is capable of hacking and planting viruses to destroy website and other portals across the world. Fraudulent transactions and online banking frauds are carried out by them by gaining access to highly confidential information as well as cyber pornography and various other crimes are committed. In simple words, no one is secure in the cyber world.

Like the conventional concept of crime, cybercrime is also an act or omission which results in breach of law and backed by sanction of the state. Two essential ingredients of cybercrimes are *actus reus* and *mens rea*. The main reason behind the growing menace of cybercrime is our heavy dependence on computers and internet. Cyber spaces have advantages as well as disadvantages. Conventional crime can be prevented to an extent by patrolling of policemen, but in the cyber space, information is open to Trojan Horses and other viruses as well as to cyber stalking and cyber terrorism. This type of crime poses a bigger challenge to the polic, prosecutors and legislators.

Statement of problem

Cybercrime is now a global concern engulfing the world. India is also not free from its clutches. It is a unique threat that is not confined to any border. It can be carried out from anywhere in the world and against any computer system. This problem has become a global issue and is becoming more difficult to bring under control.

Objective of the study

The researcher has undertaken this topic to analyse the law of cybercrime in a comprehensive manner and achieve new insights to it. The main objectives of the present study are under:

- To understand the basic concept of the cybercrime and forms of cyber crimes
- To analyse Indian cyber crime
- To decipher as to how the issue of cybercrime has been dealt with in the Indian scenario;
- To point out the possible defects in the existing law relating to cybercrime;
- To suggest the reform and remedial measure for the prevention and control of cybercrime.

Scope and limitation

The scope of the study is to do a detailed study of cyber crimes, their magnitude and nature and throw light on who are the ones responsible for it. The researcher will also analyse the success and failure of the efforts taken by India in combating this type of crime. Efforts will be made to analyse the law as laid down in the IT Act, 2000, its implementation, shortcomings and efforts to repair them as well as referring to the ITAA, 2008. The researcher will also compare the selected provisions of Indian legislation with that of US and UK wherever necessary. The only limitation of this paper is that it covers only the laws of India and only two other developed countries i.e. US and UK.

Hypothesis

The hypothesis of this paper is that cyber security at national level is poor and inadequate. The cyber space is not adequately protected. A huge number of population is present in the cyber space every moment and are using very well developed complicated technologies. Developed technologies require developed protection mechanisms. This demands for having comprehensive and effective laws and regulations for the protection of the population from the various cyber crimes. It would be effective to have a universal legal framework accepted globally since

cybercrime does not have any boundary. The legal framework should also be backed by the specialized enforcement mechanisms.

Research question

1. What is the concept of cybercrime ?
2. what are the Indian laws dealing with cybercrimes?
3. Whether the Indian laws are efficient as compared to those of developed countries like US and UK?
4. What are the possible reasons behind the increasing number of cyber crimes against individual, government and legal entities?
5. Whether the existing legal framework is sufficient enough to keep the cybercrimes under control?
6. What measures are necessary to combat cybercrimes?

RESEARCH METHODOLOGY:

The researcher has undertaken a doctrinal method of research for the purpose of this paper. The researcher has made use of primary as well as secondary sources of research like books, articles from journals, articles from newspapers and law dictionaries.

LITERATURE REVIEW:

- **Anirudh Rastogi, "Cyber Law- Law of Information Technology and Internet" -**

In this book author analysed and provided critique of laws relating to IT and different kinds of cybercrime in India. It also covered IT Act together with laws which governing jurisdiction, e-contracts IPR end E- evidence. This book also includes emerging fields of study and issue such as state surveillance, cloud computing, virtual currencies and social media regulation conditions and terms of the website, and e-governance.

- **Mohak Rana, "Crimes in Cyberspace: Right to Privacy and Other Issues"-**

This article deals with meaning and types of the cybercrime in India as well as US and UK. Also discuss about the evolution of the cybercrime, cybercrimes' categories, Indian prospective of cyber space law and cyber space crime, different types of liability under IT Act and cases of cyber crime in india.

- **Talat Fatima, "Cybercrimes" -**

In this book Dr. Fatima (i) highlights the novel issues the legal world faces in current cyber-age. (ii) Identifies online crime offences; and (iii) Analyze the legal problems and the arraignment measures for cyber criminals;. The book extensively analyses and discusses the cyber laws and judicial practices in India alongside those of the United Kingdom and the United States.

- **Vakul Sharma, "Information Technology- Law & Practice"-**

It has been written lucidly with examples, anecdotes and diagrams, which the readers may not find in any other book of this genre. This book also discusses the different challenges and aspects of the IT. And issues related to the cybercrime, Internet blocking, virtual currency, child pornography, cyber terrorism, cyber security and social media covered in legally, Also covered international prospective of jurisdiction and other issues.

- **Talwant S. "CYBER LAW & INFORMATION TECHNOLOGY"**

An AD&S Judge has made a discourse on harmony between law enforcement agencies and the computer professionals. According to the author, both are very important for securing a strong cyber security regime in the country and make cyberspace safe. The author has also made comparative study on the law definition in US and India.

TENTATIVE CHAPTERIZATION

Chapter I-Introduction

Chapter II-Concept of cyber crime and types of cyber crime

Chapter III- Analysis of Information Technology Act, 2000

Chapter IV- Cases related to cyber crime in India

Chapter V- Analysis of Information Technology Laws of UK and US

Chapter VI - Conclusion and Suggestions

CHAPTER II

CONCEPT OF CYBERCRIME AND TYPES OF CYBER CRIME

Social networking sites have been very popular right from the beginning of the new millennium. These sites provided space for many to relax, connect with old friends and also get new also.[1] But the cyber-criminal organizations have sadly misused these sites to serve their criminal acts. In the past couple of years, people started spending more time on these networks as the populations are gradually dependent on them. In the digital era, information technology growth influences the lives of people all over the world. Day after day, modern inventions and discoveries have broadened the science spectrum and created new problems for the legal community. With the rapid development of this technology leads to the commission on cyber space with emerging different types of new cybercrime today, which has also been a topic of global interest in the future.

In the cyber world era as computer use became more widespread, the rise of technology also grew, and people became more familiar with the word 'cyber.' The evolution of IT gives rise to the "cyber space" in which internet provides all people with equal opportunities to access information , analysis, data storage, etc. by using high technology.[2] Such offences are like the assault on people, companies, or governments' guarded records. Such types of attacks don't exist on the physical body but on virtual body, either personal or corporate.

Technology has exploded into communities, businesses, and individual's life over the last two decades, altering the way people study, work and interact . People in different parts of the world can connect on a range of devices , such as computers, cell phones or tablets in real time.[3] A text message, photo, video, or email exchanged by a single person can be seen by hun Dreds users in a couple of seconds, and can go viral. The IT has now become a modern tool for harassing,, doing misconduct or bullying, manipulating and harming others.

---

[1] Dr.S.V.Joga Rao "Law of Cyber Crimes and Information Technology Law", p.109 (2nd ed. 2009).
[2] Farooq Ahmad, "*Cyber Law in India- Law on Internet"*, p. 367, (2nd ed. 2008) .
[3] Saraswathi Murali, " Information Technology Handbook", p.234, (2003)

Through a socio-cultural viewpoint, there is a negative distinction between the limitations of machine criminal activity of environmental (computer availability) and societal (norms, legislation) which is a direct consequence of technology globalization. Despite having a major impact on daily life through computers and the internet, the truth remains that only a small percentage of people understand what the computer and the internet are all about?[4] Systematic analysis is required which discusses in detail the basic concepts of cybercrime, cyber space and types of cybercrime.

CONCEPT OF CYBER SPACE

William Gibson first used the phrase 'cyber space,' which he later defined as "an evocative and essentially meaningless" buzzword that could act as a code for all of his thoughts of cybernetic (transforming a text to hide its meaning). Now it's used to explain anything related to computers , IT, the internet and the complex culture of the internet. Also referred to as 'Cyber Space' is the cyber environment in which all information technology Driven contact and actions take place. Cyberspace can not be placed spatially. It's made of intangible objects like the website, forum, social networks, personal information, reputation and email addresses. Cyber space can be called an online global community with quick connectivity and no territorial barriers.[5]

Cyber space is the interactive system of computer networks where online communication takes place between the people and where people can communicate, exchange ideas, transfer knowledge, provide social support, perform business, create artistic media, direct actions, participate in political dialogue, etc.[6] Cyberspace, the modern frontier, is mankind's shared heritage, but sadly certain people exploit the common heritage and thus cyberspace is indeed a new frontier with various forms of crime. Now it's used to explain anything related to computers, IT, the internet and the complex culture of the internet.[7] The people participating in cyberspace are recognized as netizens by the fusion of two terms 'Net' and 'citizen.' Whereas Netizens implies any person affiliated with the use of Internet, computers, IT.

---

[4] S.C. Sharma, "Study of Techno- Legal Aspects of Cyber Crime and Cyber Law Legislations", p. 86, (2nd ed. 2008).
[5] Anirudh Rastogi, *Cyber Law- Law of Information Technology and Internet*, p. 2 (2nd ed. 2014).
[6] Jyoti Ratan, *Cyber Laws & Information Technology*, p. 48. (3rd ed. 2017)
[7] *Ibid.*

Webster's Dictionary explain the Cyberspace, it is the electronic structure of computer, bulletin board, interlinked networks that is considered to be a boundless world providing access to information, digital networking, and a type of virtual reality in science fiction. Cyberspace means that "the notional environment in which electronic communication occurs or virtual reality" F. Randall Farmer and Chip Morningstar defined cyberspace, by the involving social interactions than by its implementation of technology.

MODERN CONCEPT OF CRIME

A functional approach is a new approach to crime.[8] Scientific progress, industrial revolution, modernization of political institutions, schooling and intellectual emancipation of the person, loosening religious hold on culture and weakening moral values have changed the trends of crime in the modern society, especially in the information society.[9]

The law differs in nature, thereby shifting indefinitely, introducing new offenses to the catalogs and updating, removing and abolishing existing ones. Astonishing changes have been made in the crime area. The growing understanding of criminality all over the world relies on the development of individuals in society. The definition of crime occurs in different ways in various countries at all times, Like if xyz crime is crime in country A, same may not be crime in country B.

The emergence of the new method of the criminality due to industrial growth and income accumulation, Dramatic advancement in the mass media has modified the definition of conventional crimes such as homicide, dacoity, kidnapping, arson, stealing, pornography, adultery, etc. both quantitatively and qualitatively, and brought new modes of crime.

NATURE OF CRIMES

In fact, most of the societies have such values, principles, practices and rituals that its participants indirectly accept as favorable to their well-being and safe growth. Anti-social behavior is condemned as infringement of these norms and customs. Human

[8] 1 R.C. Nigam," Law of Crimes in India", Principles of Criminal L*aw*, p. 3 (1st ed. 1965).
[9] Talat Fatima, *Cyber Crimes*, p. 61 (2nd ed. 2016).

activities prohibited by Penal Law and prosecuted by State by Criminal Law shall be regarded as crimes. There are many human behaviours in our society some are forbidden by civil law, criminal law and moral code, crimes and those not forbidden by these are not wrong. The evolving character of crime can be understood as follows:

Crime is a public wrong according to Blackstone. He describes crime in two ways: first, criminality is an act committed or excluded in violation of public statute that forbids or commands it. We cannot support this concept in its entirety because Administrative Law and constitutional law etc. are infringements of public law but are not crimes. Second, he modifies his definition of crime and states a crime is a breach of the duties of public rights owed to the society as a whole, regarded as a community.[10]

Editor of the Blackstone's Commentaries, Stephen, further modified the aforementioned definition and said "a crime is a violation of a right, considered in reference to the evil tendency of such violation as regards the community at large."[11] He further added that an act is crime if it is forbidden by the law and against the societies' moral sentiments.

Secondly, Crime is social wrong. John Gillin describes criminality as an act which has been proven to be objectively detrimental to society, or which is considered to be harmful socially by a group of individuals who have the ability to impose their views, and which puts such activities under the prohibition of constructive sanctions.[12]

Thirdly, crime as conventional wrong. According to Edwin Sutherland Crime as criminal conduct in contravention of the law. Doesn't matter what the degree of immorality, unless the legislation forbids it, it's not a crime.

[10] William Blackstone, *Commentaries on the Laws of England,* vol. IV, p. 5, *available at:* http://www.ijlp.in/ijlp/imageS/Volume%20-1,Issue-1(1),%20Mar-14.pdf last accessed on 12 april 2020.
[11] Kenny, *Outlines of Criminal Law*, p. 532 (18th ed. 2013).
[12] Dr. K.N. Chan Drasekharan Pillai, *General Principles of Criminal Law*, p. 6 (2nd ed. 2020)

Fourthly, crime is procedural wrong. According to Austin "wrong which is pursued by the sovereign or his subordinate is a crime. A wrong which is pursued at the discretion of the injured party and his representatives is a civil injury."[13]

Fifthly, crime as legal wrong, according to the Halbury, crime can be understood as illegal activity which is offence against the society, and wrong doer is liable for his act for legal punishment. [14] According to the section 40 of the IPC offence means which is punishable under this Act.

FUNDAMENTAL ELEMENTS OF CRIME

To prove anybody whether he/she guilty of any offence under criminal law, evidence of *Actus reus* and *Mens rea* have to show except in strict liability crimes. Initially in Europe wrongdoer were inflicted with many charges, they did not considered the *Mens rea* as important element. But later on development in criminal law, before imposing any punishment, they start consider both *Mens rea* and *actus reus*. And acts reas must be proved beyond the reasonable doubt.

Initially crimes were simple and in very limited nature so that time criminal law was also plain. After 13th century some cases of serious offence came they led to first distinction between trot and crime. With criminal liability moral blame was linked. By this change mental element in liability got recognition.

There are two important element of crime namely

1. ***Actus reus* in Cyber Crimes**

Actus reus defined as "such result of human conduct as the law seeks to prevent"[15] in cybercrime *actus reus* is highly varied and dynamic. In simple word *actus reus* means result of human conduct.it does not include mental element. it does not limited an act only , but also includes state of affairs.

C.J. Smith & B. Hogan found *actus reus* to be a product of human action because the law attempts to prevent it. Simply guilty intent is not adequate to resolve the criminal fault but any act or omission is required to complete the offence. In in cybercrimes,

[13] Austin, *Lecture on Jurisprudence*, pp. 249-253(1920).
[14] Kenny, *Outlines of Criminal Law*, p. 532 (18th ed. 2013).
[15] J. W. C. Turner, *Kenny's Outlines of Criminal Law* , p. 17(1st ed. 1966).

Actus reus has become a challenge because whole act is committed in the intangible surroundings. the offender may leave some sign in the computer Although it becomes a huge challenge to prove in the court of law , as it is needed to be in the physical form or in that form in which they becomes admissible in evidence.

In cybercrime it easy to find the *actus reus* but very hard to prove. The act can be considered a crime may be said to have happened when a person makes use of computer function; or trying to obtain access from the internet or sending signals via different computers.[16] In cases of rape, an important feature of the *actus reus* is absence of the consent on part of prosecutor. If the prosecutor can not show this denial of consent then the *actus reus* of accused does not prove and the case will lose here. In this context we can say that *mens rea* also forms part of *actus reus*.

2. *Mens rea* in cybercrime

According to the current jurisprudence crime can be committed with *mens rea. Mens rea* is second basic factor that constitutes crime, sometimes referred to as 'a guilty mind.' definition of *mens rea* underwent a gradual shift before modern criminal law came to accept as often necessary a guilty mind of some sort or some such mental feature. [17]*Mens rea*, refers to the individual's thematic intention to commit the act. The act remains same although the state of mind causes the act 'reus' and therefore an offence. Quick all crimes need evidence of some kind of a mental dimension. many courts held that 'primarily all crime exists in the mind' Each offence requires a clear state of mind reflected by the terms in the particular section of the law: 'recklessly', 'with intent', 'maliciously', 'wilfully', unlawfully', 'knowingly', 'fraudulently', 'dishonestly', 'corruptly', 'knowing or believing', 'allowing' and 'permitting' Expressing different mental states which differ from one another. However, the basic tenets of criminal liability are motive, recklessness and knowledge.[18]

It consists of a large number of different mental activities such as recklessness, negligence, intention etc. word intention is used for a man's state of mind not only because of his ability to predict but also because it contains the expectation of the future result of his actions, as it is rightly believed that there can be no intention

[16] *Ibid*.
[17] J.C. Smith and B. Hogan, Criminal Law, p.103 (1st ed. 1988).
[18] Talat Fatima, *Cyber Crimes*, p. 70 (2nd ed. 2016).

unless there is foreseeability. When a man decides to do particular act, then he must have fair foresight of the consequences of such an act. There are no criminal liability under the Common Law for any damage or injury caused by a individual without conduct or any intention which is not unexpected.

Mens rea has been accepted as an integral component of crime except in criminal offences where there is a strict liability. Since the rise of e-crimes, the legal community is facing the challenge of defining *mens rea* in cybercrimes, in addition to many others.[19] As an important component for deciding *mens rea* in cybercrime, the offender's part is that at the time of causing t computer to perform the task, he / she must be informed that access intended to be obtained was not lawful. There must be intention on the part of hacker to secure access, although that intention may be directed with any computer and not with a particular computer. Therefore the hackers does not need to be aware of exactly which computer he / she was attacking. There are two important ingredients that make up the *mens rea*, in hacking, 1) access intended to be protected must've been unauthorized, 2)as there should be knowledge on the part of hacker regarding the access.

The mens rea requires two important elements in the case of cybercrimes. 1) 'Intention to secure access to the any software or data stored on any computer, computer network or computer system must be made. 2) The individual must know that access he intends to obtain is unauthorized at the time when he commits *actus reus*.[20]The nature and skilled involved in the cybercrime such that current legal framework couldn't do much to handle and contain same thing. In addition, the cyberspace technology has greatly eroded conventional legal principles such as property and impacted the rules of evidence such as the *locus standi*, burden of proof, and *'mens rea'* concepts.

[19] J.C. Smith and B. Hogan, Criminal Law, p. 103 (1st ed. 1988).
[20] Vakul Sharma, Information Technology- Law & Practice, p. 135, (5th ed. 2016)

CRIMINAL LIABILITY UNDER CYBER CRIMES

Crime's nature and concept has clearly established that there are two aspects of crime one being *mens rea*, and another being *actus reus*. To enforce criminal liability as white collar crime, counterfeiting coin, false evidence, false evidence etc. on the offense against State *actus reus* is sufficient. the general principle under criminal law is that unless the prosecution proves it beyond reasonable doubt person can't be convicted and the criminal law should prohibits his act or omission. The offender shall be liable for same if he has a given state of mind regarding the crime committed. The *actus reus* without *mens rea* is therefore deemed not to be a crime, and vice-versa.[21]

In the case of cybercrime, proving all aspects of Crime is very difficult. In the case of cybercrime, proving all aspects of Crime is very difficult. *Actus reus* of the cybercrime is very varied and dynamic.[22] For example , when any person starts using a mouse and keyboard to work with a computer and attempts to access the information on the others computers without his permission, there is presence of *actus reus* in the cyber space that the law seeks to control.

In a debate about whether a new law is required to deal with this emerging type of crime, cybercrimes have set in. The order school gives some creditability to the peculiar existence of new technology and peculiar set of problems unfamiliar to current criminal jurisprudence, such as scope and nature of cybercrimes, intention and difficulty in identifying the accused, jurisdiction and compliance. It contends that for dealing with cybercrimes requires a new comprehensive legislation.

Two approaches should be implemented to combat cybercrimes: firstly, crime related to computer must be treated as both conventional crime and current crimes committed through the use of high-tech technology, secondly, crime related to computer must be viewed as a crime that is special in nature and requires new legal structure.

---

[21] Dr. Vijaykumar shrikrushna chowbe, " The Concept of Cyber Crime:Nature, Scope", p. 15, 21 february (2011) SSRN,

[22] M. Dasgupta, Cyber Crime in India- A Comparative Study, p.8 (1st ed. 2009).

MEANING AND CONCEPT OF THE CYBER CRIME

The word 'Cyber,' whose usage became common in the 1980s, emerged many decades earlier since Norbert Wiener coined the word 'cybernetics' in 1948 and defined same as 'studying message as a method of controlling society and society.'[23] In reality, the phrase 'cybercrime' is mostly used in knowledge society of the 21st century, and is created by combining two terms cyber and crime. The term cyber signifies the cyber space, and it means the computer-modelled information space in which there are different objects or information of symbols image exist. It is, therefore, the place where computer programs operate and data processing takes place.[24]

Cybercrimes are nothing but real-life crimes perpetuated in digital medium and thus there is little distinction between the concept of a crime in the cyber world and the real world. The only difference is medium of crime. Cybercrime is ' 'transnational or international' – there is no border in cyber world. Computer crime, cybercrime, electronic crime, e-crime or hi-tech crime typically refers to illegal activity in which computer or network is source, device, target or crime location as well as conventional crime through use of technology such as , Internet fraud, child pornography.

Broadly cybercrime means an act or omission, which committed on through internet connectivity, may me directly or indirectly, this is forbidden by any statute, and for which corporal and/or monetary punishment is given.

DEFINITION OF CYBER CRIME

The term 'cybercrime' as a generic term that refers to all type criminal activities perpetrated through the use of computers, the Internet on the cyber space and the www. In India, in no law has any definition of the term 'cybercrime' been given yet. In addition, the IPC 1860 does not at any time use the word 'cybercrime. Even after 2008 amendment cybercrime is not define under Act. "In absence of a specific definition of notion of 'cybercrime' in European Union's legal system, a range of steps proposed in the Strategy to tackle 'cybercrime' (such as initiatives to improve cooperation

[23] Dhawesh Pahuja, "Cyber Crime & the law", Legal India, July (2011) last access on 20 may 2020.
[24] Jyoti Ratan, *Cyber Laws & Information Technology,* p. 62. (3rd ed. 2017)

between law enforcement agencies) are not explicitly related to concrete and well-defined offences."[25]

Cybercrime can be defined as any unlawful act promoted or facilitated by the computer, whether computer is object of a crime, a repository of evidence relating to a crime, or an instrument that used commit a crime. In plain language cybercrime means crime engaged in computer network or computer. But in such simplistic and limited terms complex nature of the cybercrimes can't be sufficiently expressed. Cybercrime, according to Pavan Duggal, refers to all activities that are carried out with criminal intention in cyberspace or using internet medium. These can be either traditional or newly developed criminal activities with growth of new medium. Any conduct that basically offends human awareness may be included in the cybercrime context.

Commit a crime with the using of computer technology is better definition of cybercrime; engaging in activities that threaten the ability of a society to maintain internal order. So this definition covers both traditional cybercrimes and the emerging ones. This also includes the use of computer technology, and not just the use of the networked computer technology.

TRADITIONAL CRIME AND CYBER CRIME

Cybercrimes, which are distinctly different from the traditional crimes, are often more difficult to detect and prosecute. Cybercrimes are perpetrated by perpetrators through small, targeted cyber threats, and large networks of commercial purposes leased, hijacked computers are used to launch significant attacks.[26] Researching on legal issues of the cybercrime in China, by Chen Junjiing concludes that such crimes are much more widespread unlike traditional crimes and these are increasing at faster rate. In addition, cybercrime harms society more than traditional crime, and is much more difficult to investigate.

Cybercrime contains any computer and network-related criminal act. In addition, cyber-crime also includes traditional Internet-based crimes. or example; telemarketing, hate crimes, fraud on the Internet and identity theft, are considered

[25] Prabhash Dalei & Tannya Brahme, ”Cyber law in India: An analysis”, 2 IJHAS, p.1, (2013).
[26] The Swedish Emergency Management Agency’s 2008 report,

cybercrimes when illegal activities are committed using a computer and Internet.[27] Cybercrime hackers are skilled criminals, disgruntled workers, professional, disillusioned youth, and state critics in contrast with conventional crimes.

The other distinction is based on evidence of crimes between these two words. In conventional crimes the offenders typically leave some traces of the crime, such as fingerprints or any other physical evidence, after or during the execution of the crime. But in cybercrimes cybercriminals commit their crime via the internet and there is very little chance of leaving any evidence. According to Forensic investigators who usually have experience of difficulty in evidence gathering for conviction of the cyber criminals because they either change their identities or do crime on the basis of the fake identities But as compared to conventional criminals, faking their age, sexuality, race , etc. is very difficult.[28]

Depending on the use of power, those two words can be distinguished. Many of the crimes such as robbery, murder, rape, etc. in traditional crimes involve use of excess force which leads to the physical injury on the person suffered. But as compared to cybercrimes there's really no requisite to use any type of force since in this crime criminals only use other person's identities in order to steal any private data etc.

RELATION BETWEEN CYBER CRIME AND CYBER SECURITY

Cyber crime

Cyber criminality is a crime involving use of the computer devices and Internet. This can be committed against private organisations, governmental, individual, group of individuals. It is usually with the intention of harm someone's reputation of someone, causing mental or physical harm , and benefit from it such as spreading hate, monetary benefits, and terror.[29] As happened in 1998, more than 800 e-mails were sent to Sri Lankan embassies by Tamil guerrillas, (Tamil Tigers.) According to mail sent by Tamil Tigers "We are Internet Black Tigers and we are doing this to

[27] Raj Samani "Cybercrime: The Evolution of Traditional Crime", The Journal of Complex Operations, p.275, (2011)
[28] *Ibid*.
[29] Cyber Crime Vs Cyber Security: What Will You Choose?; Europol; https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose Last accessed on 15 may 2020.

interrupt your communications." Intelligence authorities have described it as the first recorded terrorist attack on computer systems in a country.[30]

The basic principle of cybercrime law is to punish, who is with criminal intentions access without authority or unlawful use of the computer systems and internet, in order to prevent damage and alteration of systems and data on it. The greatest threat of cybercrime, however, is to an individual's financial security as well as government.

Cyber security

Cyber security is strategy against unauthorized access or threats to computers, programs, networks, personal data, etc. This is an activity which protects and defends information and communication systems against who is to be authorised to use or alteration or device exploitation. Cyber protection is often referred to as security in information technology.[31] It involves the techniques to protect networks computers, data and programs from access, which does not have authorisation or attacks that can harm or manipulate them in some way. Cyber security is basically a technical approach to safeguarding systems from such attacks.

All threats to computer system or network and all vulnerability by good cyber security recognize. It identifies the cause and fixes, as well as ensuring system security. Strong cyber security systems are focused on a blend of human and technical elements.[32]

[30] Pravin Karna "Cyber law & Cyber Crime The Concept of Cyber Crime: Nature, Scope" SSRN 2011,

[31]Robert Roohparvar, Elements of cyber security by; InfoGuard Cyber Security; Dated: 02.03.2019; < http://www.infoguardsecurity.com/elements-of-cybersecurity/> last accessed on 1 May, 2020

[32] *Ibid*.

Differences between Cyber Crime and Cyber Security

There are a few aspects that can be differentiated on cybercrime and cyber security, these are:

Types of crime:

In cybercrime- the main target in the cybercrime is individual or group of people and their data, Governments and organisations may also be the victim of cybercrimes (hate speech, trafficking, trolling, child pornography, cyber bullying)[33]

In cyber security- Such crimes are where the main target is computer network or computer software or hardware (viruses, worms, distributed denial of service attacks, ransomware)[34]

Victim: in case of cybercrime victims are individual, group of people, may be family, government or organizations or corporation. In in cyber security organization and government, so range of victim in cybercrime is wider.

Area of study: under cybercrimes Psychology, Criminology, Sociology are addressed. And how crime is committed, and what are the reason and how can be it prevent. On other hand cyber security for making network secure deals with computer engineering, Computer science, IT, Networking, Coding, and engineering strategies.

ELEMENTS OF CYBER SECURITY

Certain elements are needed to build a strong cyber security system. The elements read as follows:

1. Application security- In business ventures essential role played by the application; that is why every organization needs to concentrate on security of web applications. The security of web applications is critical for protecting customers, their interest and information. Application security helps curtail any

[33] Understanding the Difference between Cyber Security and Cyber Crime; Privacy International <https://privacyinternational.org/explainer-graphic/2273/understanding-difference-between-cyber-security-and-cyber-crime> last accessed on 1 may 2020

[34] Roderick S. Graham, "The difference between cyber security and cybercrime, and why it matters" The Conversation; < https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654> last access on 2 May 2020.

attempts to break the authorization limits set by network security policies or computer system.[35]

2. Information security- intellectual property, business records, customer data, personal data, etc. Information included. It is therefore important for a company to have very strong cyber security for data/information in order to avoid leakage.

   Security of information involves the safeguarding of sensitive information from unlawful access, use or other damage. This also means that critical data will not get lost if any problems such as malfunction of system, natural disasters, fraud or other potentially harmful circumstances occur. Integrity, confidentiality and availability are the characteristics which define information security. Data privacy , data quality, data reliability and Data confidentiality, are all part of information security.

3. Network Security- Network security is about safeguarding network and data usability and reliability. Network penetration test is performed to evaluate vulnerabilities within a system and network.

   This applies to broad variety of security policies to thwart and track unauthorized access, abuse, computer device harm and other network structures. Network protection extends coverage across companies and organizations, to multiple computer networks covering private and public communication systems.

4. Business continuity planning- Its aim is to prepare for any form of intrusion or cyber threat by detecting timely threats to systems and evaluating how they could impact the operations and methods to combat that danger. This also called as Disaster Recovery.
5. Operational security (OPSEC)- it is used for protecting functions of the organisation. This defines essential information and properties in functional system to monitor the risks and vulnerabilities.
6. End-user education- Training their employees about the cyber security is critical for an organization, since data breached caused due to the human error. Each employee must be aware of and have knowledge to deal with the common cyber threats.

[35] *Ibid*.

Training can help management to get used to and threats to system users and training of user will help eliminate resistance to change and improvements and lead to closer user scrutiny.

7. Leadership commitment- In order to have a good cyber security system it is necessary to have leadership involvement in companies and organisations. The management, implementation and development of cyber security processes without having leadership in team is complicated.

TYPES OF CYBER CRIME

We can see every day cases of cybercrime increasing and figuring out what is traditional crime and cybercrime,, is quite difficult. However cybercrime can be categorized and discussed under following heading to tackle this challenge: cybercrime against 1) against person 2) against the property 3) against the government 4) against the society.

1. CYBERCRIME AGAINST THE PERSON

Cybercrime against persons committed. This form of offences directly influenced the individual's personality. Following are the cybercrimes of some kinds that threat the user.[36]

Harassment via E-Mails- This form of harassment is very popular by file attachments, sending letters, & links, i.e. through e-mails. Harassment is growing nowadays as the use of social media sites. like Twitter, Facebook, orkut, instagram, etc. day by day increasing.

Cyber-Stalking- The phrase derives from the term 'stalking,' which means following a person to embarrass or harass that person. If computer or email is used for commit stalking.

It is often achieved by using certain criminal activities such as abuse of identity, extortion, defamation, spoofing etc. Cyber stalkers may create fake websites, create fake forums, send threatening spam, make fake profile or send harassing mails for stalk another person.

Cyber Defamation- for causing defamation Injury can be done through oral or written words, or through signs or visible representations. The person making that defamatory comment must be intent to lowering the image of person about whom the accusation was made in general public's eyes.

[36] Prabhash Dalei & Tannya Brahme, Cyber law in India: An analysis, 2013. IJHAS, volume 2, issue 1

If anybody publishing any defamatory statement by using cyber technology by like website, email or any social site may amount to cyber defamation

Hacking- In simple language hacking means accessing in computer for which you are not authorized.

Hacking isn't necessarily a crime because when a hacker is permitted to access computer networks lawfully called "ethical hacking". However, hacking crosses criminal line after computer network of someone is accessed by a hacker without their permission or authority.

Cracking- it is an act of without my consent or knowledge breaking into the my computer system and he tampered with the confidential information or data.

E-Mail Spoofing- Here an attacker steals another person's identity in form of a cellphone number and receives the SMS from the victim's cellphone number via internet and receiver. It is a very dangerous cybercrime against any human**.**

Carding It means fake credit and Debit cards used by offenders with Draw money from the bank account of victim for their monetary gains. This type of cybercrimes often includes illegal use of ATM cards.

Child Pornography- Defaulters in this cybercrime create access materials or distribute that exploit the sexual exploitation of minors. This is classified among India's most heinous type of cybercrime

Phishing- Phishing is financial crime in which criminal acts as a legitimate individual and sends an email demanding that person update his records or may be confirm details of his credit card and acquires confidential personal information.

2. **CYBERCRIME AGAINST THE PROPERTY**

The second category of the cybercrimes is cybercrimes against property, including computer vandalism, harmful program transmission, unlawful computer trespassing

through cyberspace and without possession of computerized information without authority.[37]

Intellectual Property Crimes- depriving owner wholly or partially of his rights is a crime if it is done unlawfully. Most common type of breach of IPR may be s copyright infringement, software piracy, patents, trademark infringement, service mark infringement and designs, computer source code theft, etc.

Cyber Squatting- It involves two people claiming the similar domain name either through claiming to have first registered the name by right to use it before other or by using something which is similar to the previous one.

Cyber Vandalism- Vandalism means intentionally damaging another's property and includes the destruction or disruption of information or data stored on a computer when network service is disrupted and stopped. These actions may take form of a computer theft, any computer component.

Hacking Computer System- Hackers target those like Popular Facebook, twitter, Instagram, blogging site via unauthorized computer access / control. These attacks were not intended primarily for financial gain as well as to diminish public image of a particular company or person. In April, 2013, hackers targeted MMM India.

Transmitting Virus: virus is a type of programs which is written by the programmers which attach to a pc or file and then transmit to other computers and files on a network in order to alter or delete it.

Cyber Trespass: it means accessing in to computer or network of someone without any right or authority of owner and alters, misuse, disturb and damage data by using internet.

3. CRIME AGAINST GOVERNMENT

Third category of the cybercrime is crime against crime government. Under this category cybercrime is deferent kind of crime. The development of internet has shown

[37] Shital Kharat, "Cyber Crime – A Threat to Persons, Property, Government and Societies", SSRN (2017).

that individuals and groups use the medium of cyberspace for international governments as well as To threaten nationals of a country. Such crimes manifest themselves in terrorism when an person "cracks" into a website run by a government or the military.

Cyber Terrorism- Issu**e** of Cyber terrorism concern both domestically and globally. Attacks on the Internet by Terrorist are by the distributed denial of the service attacks, hate emails and hate websites, attacks on the sensitive computer networks etc. Cyber-terrorism practices threaten the nation's security and dignity.

Cyber Warfare - It refers to hacking which is politically motivated for espionage and sabotage . It is often seen as an analogous type of information warfare to conventional warfare however this analogy is controversial both for its political motivation and for its accuracy.

Distribution of printed software- This includes distributed "printed software" from one device to different with the purpose of destroying government data and official records.

Possession of unauthorized information- Using the Internet, it is quite easy to obtain any information by terrorist and to hold that information for religious, financial, political, ideological purposes.

4. CYBERCRIME AGAINST THE SOCIETY

This is fourth category of crime. If an crime is done with intention of causing harm via using cyber means to the society at large or number of the people.[38]

Child Pornography- It involves using computer network to develop, access or distribute materials that exploit the sexual abuse of minors.

Financial Crimes- Phone networking and network sites where the offender will attempt to attack by sending false mails or messages via the internet, like using credit cards by illegally obtaining password.

[38] 3 Harpreet Singh Dalla & Ms. Geeta, "Cyber Crime – A Threat to Persons, Property,Government and Societies", ARCSSE 2013.

Forgery- This means deceiving large numbers of people by sending threatening mails, since online business payments are the normal lifestyle requirement of today.

CYBER CRIME DURING COVID -19

Most of the countries are affected by the covid-19 till now more than 50,000 people are infected. Due spreading risk government of India announced lockdown for the whole country which started from 25 March, 2020 in starting phase of lockdown all private or public companies are closed. Employees suggested to do work from home. Companies' security is at risk as all the data like financial details, customer information, trade secrets, and all other business confidential information can be accessed by click of a button to employees from their homes. To avoid misuse of the data or loss of confidential information, it is important for the employees to take special care of the data of the company and protect it from family members and friends. In addition to company information, an individual's personal confidential and financial information is also at risk given the increase in the cyber-attacks.[39]

Covid-19 and Malware, Spyware, Ransom ware [40]

Virus Attacks ,During this lockdown period , people access websites on social media such as twitter, Facebook , instagram, more frequently than watching series and movies by subscribing to the web channels such as Amazon, Netflix , Zee 5, HotStar etc. and even indulging in the online games by downloading various applications. Both of these practices are internet-based. People have to provide and/or offer permissions to readily access their personal details on their mobile, tablets, computers, and social media pages in order to use services offered by applications. Many times, users share financial information too in order to purchase applications or access online services. Citizens are becoming more dependent on different payment gates to pay their electricity bills, recharge their cell phones, purchase online essential goods and medicines, and participate in the various online activities of this nature. All those activities opened the door to attacks on ransom ware and spyware. A spyware steals the user's confidential personal data thus, ransom ware monitors a person's username and other important credentials. Such attacks could lead to losses

[39] Kiratraj Sadana & Priya Adlakha, "Cyber Crime During Coronavirus Pandemic", Mondaq (2020).
[40] Dr Mohan Dewan "COVID 19 Lockdown: Increasing Cyber Crimes in India", Lexology 2020.

not only economically but also otherwise for people. Different agencies recommend other counter-measures and safe activities that can be followed to prevent these attacks. Secured apps and Operating systems are sending its users regular updates to address security vulnerabilities and to provide additional security.

Phishing Attacks and other banking related fraud-

Banks currently operate with limited sources, & people are recommended to use online banking or telephone banking to take advantage of banking services. Cyber criminals make phishing calls or SMS massage or send phishing emails to customers of the bank claiming to be officials of bank and demanding confidential details, such as their a/c number, debit or credit card number, OTP, CVV etc. Recently, in compliance with the RBI's COVID 19 regulatory plan, banks have allowed a moratorium by postponing payment of Term Loan/EMI Instalments & Interest for 3 months. Cyber attackers are now contacting loan holders on pretext of negotiating the postponement of payment of EMI and requesting them for sharing CVV, OTP, PIN or password relevant to their accounts in order to make use of moratorium facility.[41]

Fake News or Rumours

Fake news or rumours that are circulating quickly throughout the country are another key concern that has arisen. Below are some instances of rumours & their side effects. in the month of March, the on social media there is one misleading information where "chicken is a carrier of Coronavirus" was declared cost poultry industry an lump sum loss of 1.6 billion rupees in a day. In another incident, an audio clip gone viral, claiming that vegetable vendors licked vegetables to spread Corona virus. The Government subsequently responded and released a statement saying the audio clip was false. There were another rumours that during lockdown period, government was going to cut pension by 30 per cent.[42]

Taking into account the rising number of the fake news, Karnataka and Maharashtra Cyber Police have agreed to take serious actions against anyone found to be spreading false and unverified information about COVID-19 on social media. It was also determined that in these situations a person found posting misinformation on the

[41]Kiratraj Sadana & Priya Adlakha, "Cyber Crime During Coronavirus Pandemic", Mondaq (2020).
[42] Dr Mohan Dewan "COVID 19 Lockdown: Increasing Cyber Crimes in India", Lexology 2020.

What's App group, admin of the group should be held personally responsible in his group for these material and will be liable under the applicable law. Together GOI, police and social media channels are taking steps to prevent the spread of rumours.

CHAPTER III

ANALYSIS OF INFORMATION TECHNOLOGY ACT 2000

APPLICATION - This Act extends to whole of India and also to offences committed outside India. There are certain exceptions to the Act as provided in the First Schedule:

a) Negotiable instrument as defined u/s. 13 of Negotiable Instrument Act (other than cheque);
b) Power of attorney defined u/s. 1A of the Powers of Attorney Act, 1882;
c) A trust defined under section 3 of Indian Trusts Act, 1882;
d) Will defined u/s. 2(h) of Indian Succession Act, 1925, including other testamentary disposition
e) Contract for sale or conveyance of the immovable property or interest;
f) Any class of transactions or documents, notified by Central Government

DEFINITION - The Act 2000 defines many important words like 'access', 'communication device', 'information', 'computer resource', 'computer system', 'data', etc. The definition of computer is given as any electronic, magnetic, optical or high speed data processing device or system which performs many arithmetical, mathematical and memory functions by manipulations of electronic, magnetic and optical impulses, including all input, output, processing facilities which are connected to computer in the computer system or network;

Similarly, 'computer system' is also comprehensively defined in the Act to mean a device or collection of devices with output , input and storage capabilities. Both 'computer' and 'computer system' have been widely defined in the Act to mean any electronic device with data processing capability, performing a wide range of arithmetical, mathematical, and memory functions with output, input and storage facilities. A very careful reading of each word of the definitions will show that a high-end electronic programmable gadget like switch, router or for that matter even a washing machine used in a network can be brought under the ambit of the definition. Similarly, the definition of the word "communication devices" in ITAA 2008 is very

inclusive covering cell phones and such other devices which used to transmit text massage, video, etc. like IPad and other similar devices. Later, words like "cyber café" was also introduced in the Act.

DIGITAL SIGNATURE – in ITAA 2008, "electronic signature" was defined but in the Act of 2000, 'digital signature' was covered in detail where the procedure to get digital signature certificate was also given, giving it a legal validity. It is defined as "authentication of electronic record" as per the procedure in Sec. 3. Sec. 3 of the Act, talks about the use of the asymmetric crypto system, the use of hash functions and Public Key Infrastructure. This is actually dependent on high level of technology, relying on specific technology of hash functions and asymmetric crypto system.

Thus, after the ITAA 2008, "Digital Signature" was renamed as "Digital Signature and Electronic Signature" giving legal validity to electronic signatures as a mode of executing signatures. The introduction of electronic signature brought about technological neutrality. It also includes digital signature as a mode of signature which is broader in range covering biometrics and other forms of creating electronic signature. In India there are some digital certifying authority of digital signature like M/s. TCS, M/s. MTNL and M/s. Safescript. I DRBT is the research wing of RBI which is Certifying Authority for financial sector and Indian Banking licensed by Controller of Certifying Authorities, GoI.

It is important to understand the concept of digital signature. Electronic signature does not mean a digitized or a scanned copy of the signature. In fact, there is no real signature of the person. It is not storing a signature or scanning a signature and sending it in electronic communication. It is process of the authentication of message as given under Section 3 of the Act.

Other simpler forms of authentication are retina scanning by biometric based, etc. these systems can be effective in the implementation of Act. But, the government still needs to evolve procedures in detailed to increase awareness about these systems by introducing necessary tools and conditions. The duties of the certificate of electronic signature issuing authorities have to be evolved regarding biometric based authentication and necessary steps have to be taken to make it user friendly without compromising security.

PENALTIES – chapter IX deals with Penalties, Compensation. It is a major step in claiming compensation, combatting data theft, security practices, etc.

Section 43 deals with penalties in case of damage to computer or computer system, etc. this is first ever provision for combating data theft issue. The IT Industry had been demanding legislation for a long time to address the issue of data theft, just like other physical theft. This section also deals with the civil offence of data theft. If a person, without the permission of owner of the computer, accesses, introduces virus, takes data, downloads copies, damages any computer or denies access to it to an authorized user, will be liable to pay Rs. 1 crore damages. It was removed by the ITAA 2008.

The interesting part of this provision is the civil liability for the offences. Criminality in offence of data theft is given under Sections 65 and 66. Spreading virus or writing a virus program, or other malware in a computer system, etc. all come under civil liability. This section defines all the words like computer database, computer virus, Source Code, etc.

There were debates about the liability of the organization which was sued for data theft. For the first few years of IT Act 2000, questions like responsibility of the owner, employee's liability, concept of due diligence, all of these were debated in court litigations like that of the Bazee.com case[43]. Thus, the need was felt to have a separate provision for corporate liability for information security and data protection.

A new sec. 43A was introduced in the ITAA 2008. It deals with compensation for failure in protecting data. This is like a watershed in the domain of data protection at the corporate level. It says that when a corporate body is negligent in the implementing reasonable security practices, affected person entitle to get damages by way of compensation from corporate body. The section explains the terms "body corporate", "reasonable security practices" and "sensitive personal data or information".

Thus, the corporate responsibility was brought into picture by the insertion of Sec. 43A., the corporate are under the obligation to adopt reasonable security measures.

[43] Sharat Babu Digumatri v. Government of NCT Delhi, MANU/SC/1592/2016

What comes under sensitive personal data has been clarified by the Central Government by its Notification of 2011 as including details of bank account, passwords, card details etc. After this, the IT industry became widely aware of data protection and data privacy.

Section 45 is the residual penalty provision which says that in case there is any contravention of rules for which no penalty is provided, Rs 25,000 have to be paid to the affected person.

On 11 April 2011, the Government of India, Department of I.T. notified The IT Rules. Anybody corporate will be considered to have complied with reasonable security practices if they have implemented such security practices and have a documented information security program and policies containing all types if security control measures at all levels commensurate with the information asset being protected with the nature of business. If there is a breach, the body corporate will be called upon to demonstrate the agency under the law that they have implemented all such information security program and policies. One standard security system is the Information Technology – Security Techniques – "Information Security Management System – Requirements", which is an international standard IS/ISO/IEC 27001.

It has become very important for not only the IT companies but also the financial and the banking sector that have huge computerized acts dealing with the public data, to implement data protection measures. In the event of a litigation where a breach has been committed and there is a claim of compensation, it is upon the body corporate to prove that the said "Reasonable Security Practices and Procedures" were implemented and all the procedure mentioned in the Rules of April 2011 have been taken.

This section is likely to create chaos as there is a need to redefine the role of top management, employee and responsibility of the employer and the in the data protection. Then there are issues of vicarious and actual liability, contributory and actual negligence of all the stake holders involved.

Another issue that has not been taken into account is that of cloud computing scenario. Many organizations handle other people's data and the information is stored somewhere else and not in the system of owner. There are questions regarding the information owners vis-à-vis information custodians and information container and

Service Level Agreements of the all involved parties. The entire scenario is still doubtful and there is no clear answer to these.

ADJUDICATION – after civil offences, the Act describes civil remedies for the same without the procedure of filing a police complaint. Section 46 lays down the procedure for adjudication. Any officer who is not below rank of Director as adjudicator to central or state govt. appointed by the Central Government. The Secretary of IT in a state is the nominated Adjudicator for civil offences of theft of data and the losses caused. This section is heavily criticized as it could not gain any popularity. In the first few years of the legislation, only few applications were made in the nation, and very few adjudications had been obtained. The first adjudication was obtained in April 2010 in Chennai in a case of ICICI Bank in which ordered to compensate applicant with wrongfully debited amount from internet banking, along with the cost and damages[44].

This section should be made popular among all and spread awareness among the public that recourse is there where one does not have to file a police complaint. Victims of cybercrime should be made aware of this procedure as most are not willing to take recourse of the police and file a case. The state should spend some time in spreading awareness on the procedure of adjudication for the civil offences. so that purpose for which this provision was made is served.

The appellate procedure and at the national level composition of the Cyber Appellate Tribunal under this process has also been given under this Act. The adjudicating officer has the powers of civil court and Cyber Appellate Tribunal has the same powers as that of a civil court under the CPC.

Interestingly, the IT Act does not define the term "cybercrime". It lists some of the cybercrime and stipulates punishments for the same. This is dealt under in Chapter IX titled "Offences"

[44] ICICI Bank Limited v. Mr. Umashankar Sivasubramanian and Ors. Petition No. 2462/2008

OFFENCES

Section 65 – this section deals with tampering of the source documents. Destroying Concealing, or altering source code of any computer when it is required to be maintained by the law is a punishable offence. The punishment stipulated for this offence is 3 years imprisonment or 2 lakh rupees or both. "Fabrication of an electronic record or committing forgery by interpolation in CD when produced as evidence in the court of law in punishable under this section"[45]. The term computer source code used in this section refers to computer commands, listing of programs layout, design, etc.

Section 66 – this section deals with computer related offences. This section also refers to the data theft that is mention in Section 43. The difference between the two is that in Section 43, it was a civil offence with compensation and damages, whereas in this section, it is the same act done with a criminal intention for making it a criminal offence. The act of data theft mentioned in Section 43, if done fraudulently and dishonestly is punishable under this sec. with 3 years' imprisonment or 5 lakh rupees fine or both. Earlier, in sec. 66, hacking was defined and was an offence.

After the amendment of this Act, data theft of Sec. 43 is given in Section 66 making the provision more purposeful. The term 'hacking' does not exist in the section now. Earlier, the term hacking was used in the section. Simultaneously, there would be academic courses on 'ethical hacking', etc. This created a very ambiguous situation wherein an illegal activity is being taught academically only with the addition of the word 'ethical' with it. The question is whether something which is an offence can be taught academically by prefixing 'ethical' to it. Then, courses like 'ethical assault', 'ethical burglary' can also be taught for physical defence. This anomaly was brought to an end by ITAA when Section 66 was rephrased by mapping it with civil liability of Sec. 43 and removed the word 'Hacking'. Hacking is still and offence under this section. Though some experts interpret it definitely according their convenience. They say hacking is for the good purpose and 'cracking' is for the illegal purpose. The technology is same. The only difference is that hacking is with the owners' consent and 'cracking' is an offence.

[45] Bhim Sen Garg v. State of Rajasthan and Ors., 2006 CriLH 3463 Raj 2411.

After the ITAA, Section 66 has become very wide to include a list of offences. The researcher will analyze the offence as mentioned under Section 66.

Section 66A lays down that, sending offensive messages via communication service which was struck down in the case of Shre*ya Singha*l.

Section 66B lays down that dishonestly receiving stolen communication device computer resource is an offence punishable with upto 3 imprisonment or 1 lakh fine or both

Section 66C lays down that identity theft like using others' electronic signature or is an offence punishable with 3 years' imprisonment or 1lakh rupees fine or both.

Section 66D lays down that cheating by personation by using computer or any other communication device is an offence punishable with either imprisonment of extending to 3 years and fine upto 1 lakh rupees.

Section 66E – Privacy violation – it is an offence if without consent person's private area publish or transmit and is punishable with 3 years imprisonment or fine 2 lakh rupees or both.

Section 66F – Cyber Terrorism – if there is intent to threaten the integrity, unity, sovereignty or security of the nation & denying access to any person who is authorized to access that computer resource or trying to access computer resource without authorization. If a computer is contaminated with Trojan horse, virus or other forms of malware or spyware, likely to cause injuries or death to a person or damage to property is an offence under this sec., punishable with life imprisonment.

The offences under the purview of Section 66 are cognizable and bailable. Presence of elements like intention, *mens* rea, knowledge, destruction, alteration, deletion in utility or value of data, all come under this Section.

Thus what constituted a civil offence under Sec. 43 has been made a criminal offence under Sec. 66, if offence committed with a criminal intention, attracting imprisonment or fine or both.

Section 67 deals with obscene material published and transmit in electronic form. The ITAA 2008 has widened the earlier section by including child pornography and by liability of intermediaries regarding retention of records are all included.

The section says that whoever publishes or transmits any material which is the lascivious or appeals to prurient interest or its corrupt the minds of those who will read the matter contained in it, is a punishable offence with 1st conviction for upto 3 years and 5 lakh rupees fine and 2nd conviction for 5 years and 10 lakh rupees fine or both.

This section has assumed great importance after the landmark judgment which was the first conviction under IT Act in India. In the case of *State of Tamil Nadu v. Suhas Katti*,[46] Accused was involved in the sending obscene messaged by using name of a married woman which amounted to email spoofing, stalking and the criminal offence according to the Section. Reliability of electronic evidences and strength of this section were proved by prosecution and the conviction was made.

Section 67A this section deals with publication in electronic form and transmission of material containing sexually explicit act.

Section 67B deals with **Child Pornography**.

Some of the acts which are included in this section are:

Firstly, when a child is depicted in a sexually explicit act, or digital images or creating text or promoting or advertising such material portraying chil Dren in obscene manner;

Secondly, facilitating online abusing chil Dren or inducing chil Dren to the online relationship.

[46] AIR 2015 SC 1523

Here, chil Dren mean below the age of 18 years. The punishment for the 1st conviction is imprisonment for maximum of 5 years and 10 lakh rupees fine. For subsequent convictions, imprisonment of 7 years and 10 lakh rupees fine.

There are exceptions to this section. Bonafide heritage material distributed for the purpose of education is excluded from the purview of this section, to ensure that distribution and printing of the ancient epics or the heritage material and academic books are not affected.

Screening photographs and videographs of illegal activities via use of internet are also covered under this section. Secondly, making MMS clippings or pornographic video or distributing such videos through cell phone or any other forms of communication by using internet also come under this sec.

Section 67C places certain responsibility on the intermediaries. The intermediaries should retain and preserve such information for such time period as specified by Central Govt. Non-compliance with this provision is an offence upto 3 years imprisonment or fine.

Section 69 – this is interesting section. It allows the govt or agencies to monitor, intercept, or decrypt any information received or stored in a computer resource according to the procedure laid down there. The power can be exercised by the govt, if it satisfied that such interception is necessary or the interest of integrity or sovereignty of India, security of state, defence of India, public order or friendly relations with foreign states or for preventing incitement to commission of any offence which are cognizable or if it is necessary for the investigation of any offence. In any case, the necessary procedure has to be followed and reasons for the taking such action has to be recorded in the writing. The intermediary shall extend the all technical support When asked to do so.

Section 69A as inserted by ITAA, vests Central govt or any officers of it, with power to issue guidelines for the blocking access to any such information through the any computer resource under the circumstances as mentioned above.

Section 69B lays down the power to authorize the monitoring and collecting traffic data or information through the any computer resource.

CERT-IN

CERT-IN is the single authority for issue of directions for blocking sites. It verifies the authenticity of complaint and after being satisfied that blocking is absolutely necessary, instructs the DoT – Latest Release Cell to block website. DoT ensures that the website is blocked and then informs CERT-IN accordingly. DGP of all states and such other agencies of enforcement could also approach CERT-IN.

The blocking of website becomes necessary for many agencies which are engaged in the different walks of public and administrative lives. The provision regarding blocking of website is given under Sec. 69 A of IT Act, relating to pornographic material on the website.

After CERT-IN blocks the website, it can be challenged if it results in breach of freedom of speech and expression as guaranteed to the citizens. However, websites which promote slander or defamation, hate content, promoting gambling, violence, racism, terrorism etc. along with promoting pornography, including violent sex and child pornography can be blocked since these cannot be included in constitutional right of freedom of speech and expression. Blocking of such websites may be "balanced flow of information" and not censorship.

Section 72 lays down the penalty for breach of privacy and confidentiality, upto 2 years imprisonment or 1 lakh rupees fine or both.

The most significant part of this Act is that its extra territorial applicability. The nature of cybercrime is global now. Fraudster sitting in one part of the world can commit any other kind of cybercrime in another part of the world. Thus, Section 75 states that the Act applies to offences committed outside India, of the contravention involves a computer network located in India.

This Act has over-riding provisions with regard CrPC. According to Section 78, notwithstanding the provisions of the Cr.PC, a P.O. not below rank of Inspector shall

investigate offence under this Act. Such powers belonged to officers not below the rank of a DSP in IT Act but it was later amended by ITAA as Inspector.

DUE DILIGENCE – section 79 discusses the liability of intermediaries and the concept of due diligence. Intermediary will not liable for any information from third parties that he hosts, if he has just limited functions of providing access to communication system on which third party information is transmitted or hosted or temporarily stored of he doesn't initiate transmission, select receiver of transmission and select or modify information contained in transmission and due diligence observed by him and guidelines followed which prescribed by Central Government.

The concept of due diligence has caused a lot of debates. It was believed to be an outcome of the Bazee.com case[47] where The company's NRI CEO was arrested for making MMS clipping of unacceptable pornographic content depicting school kids available for sale on public domain website he owned. In this case, there was extensive discussion on the extent of responsibility of the content provider and the ISP and what is due-diligence he should have exercised, as CEO of company.

After ITAA and the introduction of "reasonable security practices and procedures", the onus on the body corporate under Section 43A, the concept of due diligence there was a new set of rules on April 2011 titled IT (Intermediaries Guidelines) Rules. As per this, "the intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty-six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes…..[48]"

In short, an intermediary will be liable for any contravention committed by any user unless he can prove that he had taken all due diligence and has not conspired or abetted in the act.

[47] (2005) 3 CompLJ 364 Del.
[48] Information Technology (Intermediaries Guidelines) Rules 2011.

Section 80 lays down the power of any PO, not below rank of an Inspector, to enter any place, search and arrest w/o warrant any person found to have been committed an act or about to commit an offence under this Act. This is a very effective provision but has been rarely utilized by the police officers.

The Act is also applied to truncated cheques and electronic cheques.

OBSERVATIONS ON ITA AND ITAA

The researcher will now discuss broader areas of omissions and commissions in the Act and the general criticism that it has faced.

Awareness: there is no provision made in the Act to create awareness. The government or investigating agency like Police department, have not taken any serious step to create awareness among the public about the provisions of the Act, which is very essential considering that there is new technology that have to be learnt by legal professionals, litigants, the judicial officers and the public at large. It is not surprising that the adjudication process is still not known to many including the investigating agencies.

Jurisdiction – the matter of jurisdiction is mentioned in Sec. 46, 48, 57 & 61 in context of adjudication process & appellate procedure and Sec. 80 lays down the power of PO to enter and search a place for cybercrime. With regards to electronic record, Sect. 13(3) & (4) discusses place of receipt and dispatch of electronic record.

There are fundamental issues of jurisdiction that still arise in many cases. If an email is hacked by someone who is a resident of another state and the act came to be known in another state, then what should be the jurisdiction? Again, if he is an employee of an MNC with branches all over India and is frequently travelling and he suspects another employee of the same firm from his branch or from another branch and informs the police that the evidence can be found from the suspect's computer system, then what should be the jurisdiction to file the complaint? Often, the investigators don't accept complaint on grounds of the jurisdiction. Thus, it is clear that people lack the knowledge that cybercrime is borderless, geography-agnostic, territory-free and

beyond all jurisdictions. People should be made aware that cybercrime happens over 'space' or 'cloud', and proper training has to be given to the concerned people of all fields.

Evidences: evidences are a main concern in the cybercrime. In cybercrime, there is no scene of crime. We cannot mark a specific place, a computer, a network, seize hard-disk immediately and seize it as an exhibit.

The evidence, the network and the devices, the files, etc. are the crime scenes in a cybercrime. While filing a cybercrime case, be it a civil case or a criminal complaint filed with the police, evidences are found in the computer system of the intermediaries or in the opponent's system too. The police is required to immediately seize the system for the evidence as it is easy to destroy such evidences. In fact, as soon as one comes to know of the seizure, he may try to destroy the evidences by removing history, formatting etc. since these are all volatile in nature.

There is no common repository of the electronic evidences in India by which in event of dispute, The affected computer can be delivered to third party with appropriate software tools who will keep it with himself the copy of the disk and return original to owner so he can keep using that and the whenever he required he can copies. For this purpose, there are tools like "EnCase" and "C-DAC" tools which are available with search features, retrieval facilities and preserving original version.

Non coverage of many crimes: India has only one legislation regarding cybercrime – the IT Act 200. Because there is only one legislation, thus, it has not been possible to include all issues of cybercrime and many crimes per se are left uncovered. Cybercrimes like cybersquatting, etc. are not covered and cybercrimes like ISP's liability in the copyright infringement, spam mails etc. are inadequately covered.

Most of the Indian corporates use Operating Systems from the Western countries and many software and hardware items are from somewhere else. In such cases, the reach of the IT Act dealing with a utility software or Operating System, is to be specifically addressed otherwise, the user may not know whether an update is downloading or spyware is getting installed, which will give rise to very peculiar situations. The Act does not mention anything about the policy government on keeping backup of

corporates in our country or abroad and Subjective legal jurisprudence over backups of such software.

One good part is that most of crimes are also covered by IPC. So even if someone escapes the ITA or the ITAA, one cannot escape the IPC.

The existing legislation is not cybercrime friendly. It is a valuable piece of legislation and notable achievement in nation's technological growth. But it is not sufficient. We should not forget that the criminals are always way ahead in matters of technology. For example, steganography was used in case of Parliament attack to convey messages (coded) between criminals. This proves that investigators need to learn more about technology. Similarly, in Mumbai attack case satellite phones were used in November 2008 after which investigators became more aware of technological perils, since until when they were just relying on cell phones or other less complicated technologies. Hopefully there will be more awareness campaigns, and govt. will be able to enact more legislation. However, it may not be enough to introduce more legislation to deter cybercrime as we know that cybercrime conviction rates are very low compared to IPC. What may act as a deterrent is the certainty of punishment and not severity of punishment. It is not number of legislations that is important but the certainty of punishment that the legislation will bring. Thus, the government should be more proactive in cybercrime cases and ensure that there is appropriate conviction.

CHAPTER IV

CASES RELATED TO CYBERCRIME IN INDIA

Bois Locker Room case[49]

Recently the "Bois Locker Room" incident has caused a wave of anger across the nation.

The incident came in to light while multiple Instagram group chat screenshots were leaked, exposing group where images of girls, under age, were shared, and the girls were objectivized and shamed using vulgar and offensive language. There have also been alleged comments and discussions about committing heinous and gory crimes toward their modesty along with sexual violence threats.

The members were teenage school-going boys who formed the group to exchange pictures of girls, many of whom were under 18.

As much as incident highlighted need for the gender education in each household, also it brought up questions about the role of the intermediaries who provide users with platforms to host these criminal discussions.

Under **Sec. 2(w)** of IT Act 2000 define intermediary as under:

"2. (w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

In some cases intermediaries is not liable if they fall under section 79 of the IT act 2000.

[49] Aman Singh Bakshi, "Bois Locker Room: The role of Intermediaries in regulation of content", Bar and Bench, 2020.

a) Where the intermediary 's function is limited to only providing access to communication system through which third-party information is transmitted or hosted or temporarily stored: or
b) Where the intermediary doesn't initiate transmission, select transmission receiver and select or change the transmission information; and
c) The intermediary shall exercise due diligence in carrying out its duties under IT Act and also follow such other guidelines as may be issued in that name by the Central Government.

However, in the view of Sec 79(3) of IT Act, this is not blanket immunity given to intermediaries, which stipulates that intermediary shall not be excluded from liability if:

a) The intermediary itself in commission of said unlawful act conspired or abetted or induced or aided ;
b) Where any data, information or communication link which residing in or connected to the computer resource managed by the intermediary, is notified to intermediary, by the government or upon receipt of actual knowledge, , is used to commit illegal acts, and the intermediary shall not immediately disable or remove access to that content on that network without in some way vitiating the proof

Division bench of the supreme court upheld the sec. 79 of IT Act, in the shreya singhal v. UOI[50] "*subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material."*

Under section 20 of POCSO Act , on intermediary there is additional duty cast to provide the relevant info and report any such offense to "Special Juvenile Police Unit," or "local police," within ones knowledge, which is child sexually exploitative. Under Section 21 of POCSO Act, failure to disclose these offences shall be liable to punish for a period that may extend to 6 months/fine or both.

[50] AIR 2015 SC 1523

In 2015, India's Supreme Court took cognizance by suo motu of letter addressed to SC by Prajwala, an NGO, raising concerns over the rampant proliferation of videos depicting sexual abuse such as child pornography/ gang rape / rape on the online platforms such as Twitter, Facebook Whatsapp, etc.

The SC thus impleaded Facebook , WhatsApp, Google, Yahoo as parties & directed that committee should be set up for advising the Court on feasibility of making sure that videos featuring child pornography, gang rape and rape, are not available for the circulation.

Its final outcome is still pending. Although there was common consensus within committee that law enforcement agencies should block the portal and websites that don't constructively censor content that portrays sexual violence.

The government then launched the cyber-crime portal to report such instances, and recommended that a DNA software's photo to block such content at threshold. It will also set up constructive monitoring tools by the deploying tools bases on Artificial Intelligence to auto-delete illegal content. The Court also proposed that such content be established hash bank which controlled by the government.

However, the GoI notified the POCSO Rules this year on March 9 with an opinion that role of the intermediaries increasing in actively monitoring content so circulated.

Rule 11 of POCSO makes it clear categorically that, in addition to reporting offense, an intermediary shall also provide to "Special Juvenile Police Unit" or "local police" or the "cyber-crime portal" the required information, along with source from where the such information may have originated.

The report shall contain the description of the computer in which that pornographic content was found and the alleged computer from which that content was obtained, including platform on which content was shown.

IT Rules 2011 *(Intermediary Guidelines)* imposes duty on intermediaries regarding due diligence , when conducting their duties, the duty to publish privacy policies, rules and regulations, and user agreements for each person's access to or use of the computer resource of the intermediary. These will notify the computer resource users

not to view, upload, host, alter, post, send, share or update any information that is prohibited in this way. SC upheld These guideline on intermediary in *Shreya singhal case* with limitation provided in the sec. 79(3)(b) of IT Act

It is not sufficient for the intermediaries in India that their hands will be clean by just washing their hand, claiming no responsibility under safe harbor clause, for crimes committed just under their noses, specifically as sexual crimes on internet are on the rise, for both minors and adults alike.

Therefore, a vital need for revised intermediary guidelines to highlight and remedy abuse of social media platforms is required.

Following various parliamentary debates in 2018 on instances of violence arising from the abuse of social media sites, the "Ministry of Electronics and Information Technology" prepared Draft IT Rule 2018 [Intermediary Guidelines (Amendment)]. Such guidelines amend due diligence standards for these intermediaries and compel them to employ automated tools to detect and delete from public access unlawful content.

The same has still not been notified, however. Nevertheless, the same shall be made toothless if role of these intermediaries is not standardized like that in the Singapore in combating virtual offences as described above. We can only hope that events such as "Bois Locker Room" and other automated mob-lynching cases will come to a halt until effective and stricter regulation is in place.

Pune Citibank MphasiS Call Center Fraud[51]

Under this case defendant defrauded with the four customers of the City bank of US. Around 3.5 lakh US Dollar transferred to the bogus account in pune . some defendants are employee of the call centre and they got confidence in the plaintiff and get their Pin numbers. After that they used these pin numbers for committing online fraud. This case raise many question about the role of data protection. Obviously the crime was committed using "Unauthorized Access" to the clients' "Electronic Account Space." So it is firmly inside the "Cyber Crimes" context. IT Act -2000 is fairly

[51] Talwant Singh Addl. Distt. & Sessions Judge, Delhi , "CYBER LAW & INFORMATION TECHNOLOGY", available on <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> accessed on april 16,2020

flexible to handle criminal elements not protected by IT Act -2000 but protected by other laws as any IPC offense committed using "Electronic Records" may be considered a crime using "written Documents." Therefore, in addition to the section in IT Act-2000, "Cheating," "Breach of Trust" "Conspiracy," etc. are applicable in the above case' Under IT Act-2000 both Section 66 and Section 43 recognize the offence. Accordingly, persons who involved are liable for imprisonment &fine as well as liable to pay compensation to the victims to up to 1 crore rupees every victim for which "Adjudication Process" may be invoked.

Sony.sambandh.com case[52]

This is the first case in which accused of cybercrime convicted in 2013. It all started after a complaint from "Sony India pvt Ltd," they have website called "www.sony-sambandh.com" that targets NRIs. The website allows NRIs to gift or deliver Sony products for Indian friends and relatives after paying for it online. The company agrees to deliver products to interested recipients. According to the case study on cybercrime, in May 2002, someone signed on to site under "Barbara Campa 's" identity and placed a Sony Color TV set and a wireless headphone. She paid via credit card number and asked to deliver the products to Arif Azim in Noida. The agency of credit card duly cleared the payment, and processed the transaction. sony has delivered the products to Arif Azim after following the correct due diligence and testing procedures. The organization took digital photos when product was deliver for the proof that Arif Azim accepting the delivery. After the completion of the transaction credit card agency informed to company by saying that this transaction happened without authority of the card holder he denied that he purchased any item form the company. Then company file formal complaint at CBI regarding online cheating, CBI registered the case under IPC sec. 418,419, 420. Matter investigated and accused arrested. According to the investigation accused was working in the call centre. CBI recovered the item which delivered to him. In this cases he plead guilty because CBI had sufficient evidence against him. Court convicted him under IPC sec. 418,419, 420. This is the first time when any accused convicted for committing cybercrime. But court took lenient view in this case because he was just 24 year old and that was his first crime. So court released him on probation. The decision is of

[52] Mohak Rana, "Crimes in Cyberspace: Right to Privacy and Other Issues", Lawoctopus on On August 7, 2014

utmost importance for the country as a whole. In addition to being first conviction in the cybercrime case, it has shown that IPC can be extended successfully to other types of cybercrimes not protected by the IT Act 2000. Second, a decision of this nature sends out a strong message to everyone that it is difficult to take law for a ride.

The Bank NSP Case[53]

One of the important cases of cybercrime is Bank NSP case, in which a bank management trainee got engaged for marry. The couple exchanged several emails using their computers of companies. After a while both broke up and girl generated fake email ids like "indianbarassociations" and sent out emails to international clients of the boy. She used a computer from the bank to do so. Company of that boy lost a huge number of clients and brought bank to court. bank was held responsible for emails sent by using system of bank.

SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra[54]

This case known as india's first case on cyber defamation. In this case In this case, Jogesh Kwatra (defendant), being an employee of company of plaintiff , began to send out insulting, obscene, vulgar, abusive, defamatory abusive emails to the his employers as well as to various subsidiaries of said company throughout world with the intention of defaming company and Mr. R K Malhotra, Managing Director of company . The complainant lodged a case seeking a permanent injunction preventing the defendant from carrying out his illegal acts by sending out insulting emails to complainant. He further argued that defendant's actions in sending emails resulted in invasion of plaintiff's legal rights. The defendant is also under an agreement not to send above-mentioned emails. In this case, Hon'ble Delhi HC allowed an ex-parte, interim injunction to observe that the complainant had made a prima facie case and barred the defendant from making such comments.

This Delhi HC's order assumes considerable significance as this is first time that Indian Court exercises jurisdiction in a case relating to cyber defamation and grants ex-party injunction prohibiting defendant from defaming complainant by sending

[53] Talwant Singh Addl. Distt. & Sessions Judge, Delhi , "CYBER LAW & INFORMATION TECHNOLOGY", available on <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> accessed on April 16,2020

[54] CS(OS) No. 1279/2001 (Delhi High Court, 2001)

abusive, obscene insulting and defamatory, emails to either plaintiffs or respective subsidiaries.

Tamil Nadu Vs Suhas Katti AIR 2004[55]

this case was related to posting defamatory , annoying and obscene, message in group on yahoo message about divorcee woman. The accused also forwarded e-mails to the victim for details via a fake e-mail ID that he opened in victim's name. The message posting resulted in unwanted phone calls to the woman, in the assumption she was soliciting. police identified the accused in the Mumbai and within next few days he was arrested by police on the basis of a complaint lodged by victim in 2004, February. He was family friend of the women and wanted to marry with her. Although she was married with another person. After took divorce from her husband accused again started approaching her. When she refused to marry him he started harassing via internet.

Court relied on the 12 witness of prosecution side and other document presented before the court. Included testimony of the owner of the cyber café and concluded the case and held that accused found guilty under section 469 & 509 of IPC and 67 of IT act.

Cosmos Bank Cyber-Attack in Pune[56]

In 2018, a very famous cyber-attack on the "Cosmos Cooperative Bank Ltd" Pune. That daring attack shocked India 's entire banking sector when the hackers siphoned off "Cosmos Cooperative Bank Ltd." 94.42 crore rupees in Pune. ATM server of bank hacked and took information of various debit and visas cardholders. These money with Drawn from around 12000 ATM of different country. And around 13.92 crore rupees were transfer to the Entity based in Hong Kong which uses the SWIFT facility. According to investigation, they used visa card for money transferring from the outside India and in India by Rupay card. FIR was registered under IPC and IT Act under different section.

[55] Talwant Singh Addl. Distt. & Sessions Judge, Delhi , "CYBER LAW & INFORMATION TECHNOLOGY, available on <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> accessed on April 16,2020

[56] Indian Express, August 11, 2018, available on < https://indianexpress.com/article/cities/pune/malware-attack-cosmos-bank-gets-rs-5-72-cr-from-hong-kong-based-bank-6273134/> last access on 23 may 2020

According to press report issued by Cybercrime department DCP police is contacting HongKong bank for 13.92 crore rupees, and police of Pune also trying contact to authorities of Hong Kong with the help of External Affairs Ministry. cosmos bank also filed civil suit in court of Hong Kong, and by the court order first instalment return to the Cosmos bank amount, 572 crore of 94 crore according to the press released. Around 18 person arrested in this case and SIT filed charge sheet of 1700 pages.

Hack Attack on Indian Healthcare Websites[57]

In 2019, Healthcare websites based in India recently became victim of cyber-attack. According to US-based firms of cyber security have reported, hackers broke into and attacked a leading Indian-based healthcare website.0d hacker stole record of 68 lakh physician and patient.

Shreya Singhal v Union of India[58]

Sec. 66A of IT Act, 2000 came into force pursuant to a 2009 Amending Act. And the plaintiff questioned the substantive validity of sec. 66A in the current writ petition. The petitioner argued Section 66A has given lead to new, incorrect forms of crime. petitioner challenges constitutional validity of Act on the ground of Art. 19(2). Vagueness of the section and Art. 19(1) (a), and there is no "intelligible differentia" mode of communication like one who uses internet or other medium of communication.

Issue was whether sec. 69 of the IT Act pass the challenge of constitutionality?

Court held that "India is a sovereign, democratic and republic country as has been stated in the preamble of the Constitution. It cannot be overemphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme. The content of the expression "freedom of speech and expression" is thus three: discussion, advocacy, and incitement. It is only when all these three contents are fulfilled that Article 19(2) is applied. Under our constitutional scheme, it is not open to the state to curtail

[57] India Today, August 22, 2019, available on https://www.indiatoday.in/crime/story/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1590345-2019-08-22 last accessed on 23 May 2020
[58] AIR 2015 SC 1523

freedom of speech to promote the general public interest. If a public order under section 19(2) is violated by a law then that law is unconstitutional and void for public order is synonymous with public safety and tranquillity. The test to identify whether the public order has been infringed or not is to ask a question: Does a particular act lead to disturbance of the current life of the community or does it merely affect an individual leaving the tranquillity of society undisturbed?"

Where no rational criteria are provided for determining liability in section that creates an offense and where no specific guidance is provided either to authorities and courts, law-abiding citizens, a section that creates a crime which is ambiguous must be struck down unreasonable and arbitrary. It is very clear that words used in the sec. 66A are entirely open-ended, ambiguous and undefined.

Moreover, a Future offender of the sec. 66A and the enforcement authorities of sec 66A have absolutely no acceptable criteria for booking a person for an offense under sec 66A. Section 66A therefore arbitrarily, disproportionately and excessively invades right to freedom of speech and upsets balance between that right and reasonable restrictions which may be enforced on that right. This Section is therefore unconstitutional on the basis that it requires with its sweepingly protected expression and expression which is innocent with nature and is thus likely to use in the such a manner as to have a harmful impact on freedom of speech and th this sec. have to struck down on ground of over broadness.

In addition, there is an "*intelligible differentia*" between online speech and other communication channels for which the law will establish different offences. Section 66A is also not discriminatory according to Article 14

And court held that sec. 66A is unconstitutional it is violate Art. 19(1)(a).

Ritu Kohali Case[59]

It was first case recorded in India against cyber stalking and this cases lead to the to amendment in IT Act in 2008. under this case one women named Ritu Kumari was stalked. Where kathuria followed the Ritu Kumari chat on social media via online

[59] Prachi Shah, "Cyber Stalking & the Impact of its Legislative provisions in India" https://www.legalindia.com/tag/ritu-kohli-case/ last access on 25 May, 2020

source and used obscene language to harass her, he also circulate her number to different men. After that she received unwarranted obscene calls at night-time , continuing for three days. Following this situation, she were forced to file complaints with Delhi police and police tracked his IP addresses after complain was file and arrested kathuria u/s. 509 of IPC and Sec. 66-A was adopted in 2008 solely because of this case.

Sanjay Kumar v. State of Haryana[60]

Manager of the "Vijay Bank, NIT, Faridabad," filed a complaint with the police asserting that Telecommunications Ltd.and M / S Virmati Software had charged petitioner for software system maintain which supplied to bank by petitioner. But petitioner has exploited computerized bank account interest entries and thus cheated complainant bank through forging electronic records for causing wrongful losses to the bank. Trial court found him guilty under IPC sec 420, 467, 468 & 471 and under IT Act sec. 65&66 with rigorous imprisonment, accused file appeal in the HC, and HC dismiss the appeal by stating that The Trial Court was fully justified in convicting petitioner, and as can be seen clearly, the learned Appellate court had made no mistake in upholding accused petitioner's conviction. The petitioner's learned counsel was not able to prove any non-reading or misreading of any evidence, and judgment of trial court was upheld.

Lakshmana Kailash K.case 2017[61]

Under this case police arrested A 26 year old engineer Lakshmana, on Auguest 31 arrested form home and wrongfully and detain for the period of 50 days, because person was mis-identified by the Airtel who was service provider, as that the person insulted the great historic person Chatrapati Shivaji bu posting some photos on Orkut, a social network site. He was identified by police based on The ip address details which acquired from Airtel and Google ISP of Lakshmana. He was transported to Pune and police detained him for 50 days before this was found that Airtel had incorrectly provided the IP address. clearly this was a mistake according to fact that

[60] 2013) CRR 66 (O&M) 1.
[61] CRIMINAL PETITION No.4617/2009

police was n't properly stipulated whether the accused person posted the contents at 1:15 p.m. while asking for information from ISP Airtel.

Verdict: State Human Rights Commission took cognizance of newspaper accounts of his plight and order subsequently that company have to pay 2 lakh rupees to Lakshmanna as damages. The case highlights how minor breaches of privacy by intermediaries and ISPs may have implications that severely undermine certain fundamental human rights

Yahoo Inc. v Akash Arora & Anr.[62]

This was the first case of cybersquatting in India. The plaintiff filed a complaint against defendants for obtaining a order of permanent injunction prohibiting defendants from carrying on business, advertising, selling in any products or services under domain name or trademark a name "yahooindia.com" on Internet or otherwise or under Any other domain name or trademark which deceptively or identical similar to "Yahoo" of the plaintiff! i.e well-known trademark ".

It was contention of the defendant that "Yahoo!" 'Domain name or trademark allegedly belonging to complainant was not registered in India at that time and therefore he could not use it as a grounds for action in the respect of infringement of the trademark

Also another argument made by the defendant that maintained that word "Yahoo!" "It is a generic term which is neither invented nor special and as such has no distinctive feature.

It was further argued that because the accused have used disclaimer all along, so there was no deceit and therefore accused can't take any action of the passing of or cybersquatting.

The Court ruled in favour of the complainant and issued injunction against Akash Arora. It was held that internet service provided by the complainant had become accepted and recognized globally. though Court agreed with contention of the defendant that the "Yahoo!t" is a dictionary word but it had gained ample

[62] 1999 IIAD Delhi 229.

uniqueness and distinctive character to prevent complainants from cybersquatting or passing off.

Mr. Arun Jaitley vs Network Solutions Private ltd[63]

Infringement of copyright, High Court of Delhi ordered the accused No. 3 to permanently refrain from using, endorsing, advertising or maintaining the domain name 'Arunjaitley.com' and to refrain from adopting, using logo, the name in any of Internet domain names where name 'ARUN JAITLEY' is features. Also ordered to transfer the aforementioned domain name to plaintiff with immediate effect by defendant no. 3 and others. It was also directed to necessary regulatory body under ICANN Rules to block such domain name and to transfer this domain name to complainant immediately and for carrying out the necessary formalities in this regard.

Sandeep Varghese Vs. State of Kerala[64]

A complaint lodged by a company representative engaged in India and abroad , in the business exporting and trading petrochemicals was filed against nine persons accusing offenses u/s 65, 66 & 66A, C , D of IT Act also with Sections 419 & 420 of IPC. "www.jaypolychem.com" was the website of the company but accused Sam made another similar website "www.jayplychem.org". Accused was dismissed from that company. Accused conspired with other co accused namely charanjeet and preeti who was relative of the accused. On the similar website accused make publish malicious and defamatory matters regarding the company and the director of the company. charanjeet and preeti had been based in Cochin and had acted in collusion with known and unknown individuals who collectively cheated company and impersonation, forgery etc. committed. Rahul and amarjeet another accused had visited Cochin and Delhi. The accused sent e-mails to defame the image and name of Company and Directors of company from fake e-mail accounts of the different clients, bank, suppliers etc. The defamation campaign conducted by all of the above listed individuals has done considerable harm to the Company's name and reputation. Company suffered losses by suppliers, producers, and consumers of several crores rupees, and was not able to do business.

[63] CS(OS) 1745/2009 & I.A. No. 11943/2009 & 17485/2010.
[64] Bail Appl..No. 2003 of 2010.

Syed Asifuddin & other v. The State of Andhra Pradesh & Another[65]

Tata Indicom employees were charged under hacking with source code of computer u/s 65 of the IT Act , for exploiting the mobile phone-programmed Electronic 32 Bit Number, that was used only on "Reliance Info Com Service Network." Any copyright infringement in the computer program is punishable u/s 63 of the Copyright Act. Hence, prima facie, when any person alters another person's computer program or another company's computer ,then it will be copyright infringement. Court held that The court held that such tampering of code amounts to tampering with the computer source code and will not be covered by fair dealing and other exceptions to copyright infringement under section 52 of the Copyright Act as it was not reverse engineered to perform the intended function it was supplied for and nor was it reverse engineered for a lawful purpose. "

Tata Indicom is also competitor according to the sec. 52 of Copyright Act, and not a legitimate processor. Since the phone has been reverse engineered with unlawful purpose of unlocking code as then it can even be used on "Tata Indicom Network," ingredients required by sec. 65 of the IT Act, 2000 were sufficient. With regard to quashing FIR , the court quash the FIR w.r.t. sec. 409, 420 & 120B but court refused to quash FIR under Sec, 63 of Copyright Act under Sec. sec. 65 of IT Act

Abhinav Gupta v. State of Haryana[66]

The petitioner has been charged with hacking his former employer's confidential documents, confidential design plans and Drawings while in its employment . He had allegedly purposely given the secret details to his former employer's competitor. The Punjab and Haryana HC dealt with this petition filed by petitioner for anticipatory bail u/s 438 of CrPC, w.r.t. of a FIR lodged pursuant to Sec. 66 of IT Act, , Sec. 420 & 406 of IPC. The Punjab and Haryana HC examined the 'hacking' definition pursuant to Sec. 66 of IT Act, and discovered from the screen shots submitted by defendants that the petitioner had transferred secret information to his private e-mail during his previous employment and subsequently disclosed the same information by forwarding it to competitor's e-mail box that he later joined. The High

[65] 2005 CRI LJ 4314.
[66] 2008 CriLJ 4536.

Court refused to consider the petitioner's claim that these material was sent to his private Id for fulfilment of his duties on ground that he would in no case have sent that email to company of the competitor where he afterwards took up jobs. The court found that accused is "hacker" who accessed information for his own financial profit or for his new employer and refused to grant the petitioner anticipatory bail.

National Association of Software v. Ajay Sood & Other[67]

in this case meaning of phishing explained by the court, as cybercrime where criminals use computer or internet to cheat gullible people through impersonating real institutions such as bank to thieve sensitive personal information like credit or debit card no. and misuse the information to make unlawful money.

Shri Umashankar Sivasubramaniam v. ICICI Bank[68]

The plaintiff filed a case for damages u/s. 43 of IT Act 2000 as he was the victim of the phishing attack through an e-mail which indicated that it has been sent through his bank demanding that his personal account data be updated When bank argued there was some negligence on the part of petitioner, Adjudicating Authority found that bank had not taken due diligence steps to protect its banking network in such a way that customer could identify the bank's mail and petitioner was granted 12,85,000 rupees as compensation. Similar to the phishing concept is 'vishing' and 'smishing.' Smishing is using sms on cell phones to make monetary gains by impersonating and cheating a legitimate service provider. Vishing is by using phone calls or voice recordings to accomplish the similar goal. However, no cases reported on these emerging concept.

[67] 119 (2005) DLT 596.
[68] Petition No. 2462/2008 dated 18.04.2010

CHAPTER V

ANALYSIS OF INFORMATION TACHNOLOGY LAWS OF UK AND US

IT LAWS OF UK

CYBERSECURITY AND THE UK LEGAL LANDSCAPE

As the businesses are expanding worldwide and digitisation of assets and operations are taking place, it is imperative to continuously assess the information technology infrastructure to safeguard important information and data.

One of the key challenges faced worldwide and especially UK is implementing cyber security measures that adequately protects against online attackers and also ensures compliance with the laws of cyber security. Situation is more complex in UK as there is no one single all-encompassing "cyber security" law in the country. There are different laws which impose cyber security obligations on all entities.

Cybercrime is a major concern around the world today. The developed countries are also not free from it even though they have well developed enforcement mechanisms. Money is being made illegally with the help of malwares and various other computer-specific crimes are committed.

COMPUTER MISUSE ACT, 1990

The first piece of legislation enacted to address computer misuse in UK was Computer Misuse Act 1990. Existing legislation for dealing with hackers was not adequate and this legislation came as a response to the same. The inadequacy of existing legislation was highlighted by the failure to convict Stephen Gold and Robert Schifreen who had gained unauthorized access to BT's Prestel service in 1984. They were charged under the Forgery and Counterfeiting Act 1981. Concerns arose when they were acquitted by the Court of Appeal and the acquittal was upheld by the House of Lords.

The Computer Misuse Act 1990 was enacted with the aim of securing computer material against unauthorized access or modification and for other similar purposes. This Act sets out three computer misuse offences:

1. Unauthorized access to computer material
2. Unauthorized access with intent to commit or facilitate commission of further offences
3. Unauthorized modification of computer material[69]

Maximum sentence prescribed for the offences is ten years for the fourth offence. The sentence for the second and the third offence is five years whereas it is six months for the first offence. The first prosecution under this Act was brought about in 1995 when an individual, Christopher Pile, was prosecuted for distributing a computer virus. He had created the virus Pathogen and Queeg. Both of these malwares implemented his SMEG (Simulated Metamorphic Encryption Generator) polymorphic engine. This made it more difficult to be detected and were designed to trash the victim's hard Drive. He placed these viruses on bulletin boards in the form of games and anti virus programs. The virus had caused damage amounting to £ 1 million[70]. He had pleaded guilty to eleven charges under Sec. 2 and 3 of the Computer Misuse Act and had ultimately received an 18 months' prison sentence[71].

Another conviction was that of a 22 year old Welsh web designer called Simon Vallor[72]. He had pleaded guilty to creating and distributing three mass mailer viruses - Gokar, Redesi and Admirer. The offence was covered by Section 3 of the Act. He was sentenced to 2 year prison in January 2003. His worms had spread to 27,000 computers in 42 countries[73].

[69] The Computer Misuse Act, 1990.
[70] Peter Victor, "Black Baron a self taught whiz kid", The Independent, 16 November 1995.
[71] *Ibid.*
[72] R v Vallor [2003].
[73] John Leyden, "Welsh virus writer Vallor jailed for two year", The Register, 21 January 2003.

COMPUTER MISUSE ACT AMENDMENTS

Most significant amendment came about in 2005 when the Act was updated to align with the Serious Crime Act 2015[74]. Computer misuse was added to the list of serious crimes with maximum penalty being increased to a prison sentence of 14 years and fine, if found guilty. If an individual is charged with an offence that constitutes a threat to the national security or human welfare in general, the sentence can be upto lifetime imprisonment.

There were subsequent developments to the Act. In 2006, Section 37 of the Police and Justice Act, 2006 was inserted in the Computer Misuse Act as Section 3A. This section classified making, supplying or obtaining any article for use in a malicious act using a computer, as a criminal activity.

PROBLEMS

Thus, the Computer Misuse Act was enacted to help deal with the problem of misuse of computers by way of 'hacking' and 'unauthorised access'.

The Act was a way forward in terms of cyber laws in the UK. However, it still had many loopholes and had failed to combat the challenges of unauthorised access gained by hackers or viruses created by cyber criminals. The case of *R v. Bedworth* [1991] proves the problem with Section 2 in proving 'intent'. This case is a peculiar example of how the offender had used the defence of addiction to counter the allegation of intention of committing the crime. He had pleaded that he had no intention in committing the crime. Strangely, even though addiction is not a defence to a crime, the jury had acquitted him as they believed that he did not deserve heavy penalty.

Another loophole that might come as a blow is that the judges might lack technical knowledge regarding the use of computers. Inadequate knowledge will make it difficult to apply the law properly and tend to make inappropriate interpretations. This problem was highlighted in *Rv. Cropp [1991]* where the judge acquitted the person on the basis of his opinion that an offence was only committed if one computer is used to

[74]Explanatory Notes , Serious Crime Act 2015 available at http://www.legislation.gov.uk/ukpga/2015/9/pdfs/ukpgaen_20150009_en.pdf> last accessed on May 25, 2020.

obtain material stored on another computer. His was not the correct interpretation and it sprung from the judges' inadequate technical knowledge about computers.

These are the problems that raise questions on effectiveness of prosecuting offenders and preventing hackers. The definition of 'computer crimes' is too broad in the Act as it simply states 'unauthorised access to computer material'. This had created problems in the case of *DPP v. Bignell [1998]*. The Drafting of the law seems very general and casual. With time, it has just become a blunt instrument when policing cybercrimes. This is proved from the fact that inspite of high reporting of crimes, there have been very few prosecutions till date[75].

SPAM, MALWARE AND THE LAW

Mostly, everybody deals with the problem of spam. The problem of spam is widespread. It does not only include inappropriate content but it is also used to deliver malicious code to the recipients. Spam messages work in a way that the recipients will open the link to the website which are infected with malicious codes by cyber criminals. This method is also used by phishers to direct victims to fake websites from where their confidential data is stolen.

To address the problem of spam, the Department for Trade and Industry introduced the "Privacy and Electronic Communication Regulations (EC Directive) 2003." These regulations exist alongside the Data Protection Act and the GDPR. These regulations protect specific privacy rights of people in relation to electronic communications[76]. They have specific rules on:

a) Marketing calls, emails, texts and faxes
b) Cookies (and similar technologies)
c) Keeping communications services secure
d) Customer privacy as regards traffic and location data, itemized billing, line identification, and directory listings[77].

[75] Michael J L Turner, "Computer Evidence" available at https://www.computerevidence.co.uk/Cases/CMA.htm last accessed on May 25, 2020
[76] PECR, available at https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/ last accessed on May 25, 2020
[77] *Ibid.*

These regulations were derived from the European Law. It had implemented the European Directive 2002/58/EC, which is also called 'the e-privacy Directive'[78].

The e-privacy Directive is complementing the general data protection regime. It also sets out very specific privacy rights of all entities in the domain of electronic communication. It very categorically acknowledges the fact that the use of computer and internet poses new threats to the privacy of people.

The PECR have been amended many times till now. Last amendment was in 2018 where cold calling of claims management services was banned. Secondly, director's liability for serious breaches of marketing rules was inserted. In 2019, cold calling of pension schemes was banned and the definition of consent was incorporated from the GDPR.

These regulations mandated that companies must seek permission before sending emails or SMS messages. The law states that no one is permitted to transmit unsolicited communications for the purposes of direct marketing unless the recipient has consented to receiving such messages.

However, there are limitations of this law. These regulations only apply to individual email addresses and not business email addresses. The penalties are also inadequate as compared to the ones provided under the Computer Misuse Act, 1990. Breach of any provision of this regulation requires reporting of the act too the Information Commissioner's Office who is responsible for deciding whether the person should be taken to the court or not.

Another serious limitation is that the legislation is only applicable to senders within the UK. Most spam originates beyond the UK (Russia and US are the top sources of spam)[79]. Thus, if this legislation is not applicable beyond UK, it is not effective against the actual spammers. This highlights a very important problem with the measures taken by the countries to combat cyber crime and deal with cyber criminals: geo-political restrictions.

[78] *Ibid*.
[79] Darya Gudkova , Daria Bronnikova, "Kaspersky Security Bulletin: Spam Evolution 2008" , March 2 , 2009.

THE POLICE AND JUSTICE ACT 2006

This Act incorporates the amendments to the Computer Misuse Act. Under Section 1 of this Act, the maximum sentence was increased from six months to two years. Section 3 of this Act originally read 'unauthorised modification of computer material'. This was changed to ''unauthorised acts with intent to impair or with recklessness as to impairing, operation of computer,..' etc. It now provides a maximum sentence of ten years.

The Act also added another section, 'making, supplying or obtaining articles for use in computer misuse offences', which carries a maximum sentence of two years.

This provision had invited a lot of criticisms. It was initially intended to make hacking tools illegal but it came to be applied to legitimate tools used illegally.

EUROPEAN CONVENTION ON CYBERCRIME

One of the most serious limitations of any cyber law is its applicability. The European Convention on Cybercrime was introduced for the purpose of providing a common framework for dealing with cyber crimes. It was adopted in November 2001 by the EU Committee of Ministers of the Council of Europe[80].

The treaty is very wide n scope and covers a wide range of cybercrime. It includes illegal access, data interference, misuse of devices, illegal interception of data, system interference, computer-related fraud, offences related to child pornography, computer-related forgery, offences related to infringements of copyright and related rights. The treaty is designed to provide a common law enforcement framework for dealing with cybercriminals[81]. It also fosters information sharing among all signatories.

However, many countries have still not ratified the convention. It is worrying because some of them are big sources of malicious code.

[80] European convention on cybercrime.
[81] *Ibid*.

PERSONAL INTERNET SECURITY

House of Lords Science and Technology Committee published a report on Personal Internet Safety in August 2007[82]. The report heavily criticized the UK government for placing the main onus on the individuals for making the internet a secure space. Internet was described as "the playground for criminals". It suggested that there are many entities which have a stake in the internet like the ISPs, police, etc. They should put in all efforts to promote personal internet security.

The Committee suggested that all parties should take utmost care to secure the internet Companies, banks, software vendors, ISPs, etc. should put every possible effort that comes under their domain, to protect the internet.

CRIME AND PUNISHMENT

It is true that only legislations are not enough to tackle the problem of rampant cybercrime unless there is adequate enforcement mechanisms to implement them. It is of utmost importance for police to have the resources to deal with the growing problem. After the Computer Misuse Act was introduced, only a very few police officials outside the Metropolitan areas had the technical knowledge and expertise to deal with the problem of cybercrime. Later, resources were put together to create a dedicated agency to deal with the problem of cybercrime.

In April 2001, the government established the National Hi-Tech Crime Unit to provide directed response to cybercrime.it worked in association with a lot of experts and specialist organizations like the National Crime Squad and the National Criminal Intelligence Service.

The NHTCU was a success. It was successful in the arrest of Russian hackers and some others who were trying to steal money from the London branch of the Japanese Sumitomo Mitsui Bank in October 2004[83].

In April 2006, the NHTCU's responsibilities were taken over by the Serious Organised Crime Agency (SOCA).

---

[82] Report on Personal Internet Safety, 2017

[83] John Leyden, "How police busted UK's biggest cybercrime case", The Register , 19 March, 2009.

In April 2007, the rules relating to reporting of bank frauds were changed. The Fraud Act, 2006 was introduced which laid down that banks and other financial institutions should be contacted in the first instance, for reporting card, cheque and other online banking frauds. The main aim of this law was to reduce the bureaucracy in the system. However, one concern of this Act was that after this there will be under reporting of frauds.

In 2009, the Police Central crime unit(PCeU) was created. This did not replace the SOCA or other police agencies. It was just for coordinating the response to cybercrime and provide a national investigative capability for the most serious e-crime incidents[84]. Then, the National Fraud Reporting Centre was introduced to provide public a way to report non urgent fraud via telephone or online[85].

Even where the law is sufficient to deal with cybercrime, it falls short because of inadequate enforcement mechanisms. Thus, mechanisms in UK have in a way been able to enforce the few laws of cybercrime that are in force there.

USING CIVIL LAW TO DEAL WITH CYBERCRIMINALS

In a paper called New Powers Against Organised and Financial Crime[86], the government proposed to fill the gaps in criminal law for catching the criminals by making use of civil courts, including the use of Organised Crime Prevention Orders. The Courts would be able to impose an order on the basis of balance of probabilities.

The proposals finally took shape in Serious Crime Act 2007, to provide the best tools for law enforcement agencies.

BALANCING SECURITY AND FREEDOM

The Serious Crime Act came as relief as it provided the police with powers 'to detect, disrupt and prevent serious crime'[87]. After this, the main concern was relating to the impact on civil liberties. This is because the burden of proof required in a civil court

[84] PCeU mission statement.
[85] *Ibid*.
[86] Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/272311/6å875.pdf last accessed on May 25, 2020.
[87] The Serious Crime Act.

is lesser than that required in a criminal court. Thus, it gives way to miscarriage of justice in many instances.

However, UK is not the only country dealing with the problem of balancing personal freedom and security. Many developed countries like Germany are also doing the same. But so far, no resolution has been made brought about in any of the countries.

Thus, this act of balancing has to be done by UK till there is a permanent solution to this.

IT LAWS OF US

Cyber security is a growing concern for the government as well as the private sector in the US. With the growth in complicated information technology regime and the e-commerce sector in the US, there is a rapid rise in cybercrimes, causing huge losses to the government and the people.

In the US, data breaches have gained particular attention due to the heavy impact on the financial, healthcare and other sectors. After the development of complicated digital platforms, data breaches have assumed new dimensions and have caused more losses than ever before.

The number of data breaches in the US increased from 157 million in 2005 to 781 million in 2015. In 2019, number of data breaches was 1473 with 164.68 million records exposed[88].

The year 2019 witnessed the largest data breach till date in US history. In 2016, Yahoo revealed that hackers stole user data and information of atleast 500 million accounts in 2014[89]. In December 2016, the company announced another hack in 2013 that affected over 1 billion user records.

[88] Clement, "Cybercrime: number of breaches and records exposed 2005-2019", Statista, (2020) available at https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ last accessed on May 27, 2020

[89] Dustin Volz, "Yahoo says hackers stole data from 500 million accounts in 2014", Reuters , (2016).

CONSUMER PRIVACY PROTECTION ACT 2017

The Act aims at protecting the personal information of customers, to avoid identity thefts and to update citizens and organisations of security breaches and prevent the misuse of sensitive information of users[90].

The Act is applicable to all institutions which access, collects, uses, stores and transmits personally identifiable information of more than 10,000 US citizens over a specific period of time. The penalties do not excess $5 million. However, if it is found that it was an intentional misuse of data, an additional $5 million can be imposed.

COMPUTER FRAUD AND ABUSE ACT [CFAA]

In 1984, the US passed the Computer Fraud and Abuse Ac. Since then, there has been many amendments to this Act. CFAA focusses on many types of computer related crimes.

This Act penalizes any conduct that attacks a computer system. It is a cyber security law of US. It protects computers connected to the internet. It protects the computers from trespassing, damage, threats, espionage, and from being misused as instruments of fraud. It is not a comprehensive law, but tries to fill the gaps of the other federal criminal laws. The CFAA focusses on the following types of crime:

- 18 U.S.C. 1030 (a)(3) – computer trespassing (e.g. hacking) in a government computer;
- 18 U.S.C. 1030 (a)(2) – computer trespassing (e.g. hacking) resulting in exposure to certain governmental, credit, financial, or computer-housed information;
- 18 U.S.C. 1030 (a)(5) – damaging a government computer, bank computer, or a computer used in affecting commerce, interstate or foreign (e.g. worm, virus, Trojan horse, etc.);
- 18 U.S.C. 1030 (a)(4) – committing fraud which involves unauthorized access to a government computer, bank computer, or a computer used in affecting commerce interstate or foreign;

[90] The Consumer Privacy Protection Act 2017.

- 18 U.S.C. 1030 (a)(7) – threatening to damage a government computer, bank computer, or computer used in affecting commerce, interstate or foreign;
- 18 U.S.C. 1030 (a)(6) – trafficking in passwords for a government computer, or when the trafficking affects commerce, interstate or foreign;
- 18 U.S.C. 1030 (a)(1) – accessing a computer to commit espionage.[91]

Subsection 1030 (b) makes it a crime to attempt or conspire to commit any of the aforementioned offences. Subsection 1030 (c) lays down the penalties for committing the offences, that range from imprisonment of not more than a year for simple cyberspace trespassing to a maximum of life imprisonment when death results from intentional computer damage[92]. Subsection 1030 (d) protects investigative authority of the Secret Service. Subsection 1030(f) denies any application to other law enforcement activities. One interesting provision is that in subsection 1030 (g), there is a civil cause of action for victims of these crimes. Subsection 1030(i) and (j) authorize confiscation of property used to commit any of the aforementioned offences.[93]

Act condemns unauthorized intrusion ("hacking") into federal government computers. The Act includes provisions which prevent attempts and conspiracies to intrude[94]. It prohibits only "intentional" trespassing.

One limitation of the provision is that it is applicable only to trespassing upon governmental computer space.

The penalties for conspiracy to violate, or for violations or attempted violations are imprisonment of not more than one year and fine upto $100,000 for first offence and not more than $250,000 for subsequent convictions[95].

Other offences attract punishments like forfeiture, money laundering, restitution, sentencing guidelines and other civil liability provisions

[91] The Computer Fraud and Abuse Act.
[92] The Computer Fraud and Abuse Act.
[93] *Ibid*.
[94] Subsection 1030 (b) of the CFAA.
[95] 18 U.S.C. 1030 (c).

ELECTRONICS COMMUNICATION PRIVACY ACT [ECPA]

The Electronics and Communication Privacy Act is another legislation dealing with crimes over wire, oral and electronic communications while being made, transmitted or stored in a computer, as well as email and data stored electronically[96].

It is a law that makes it illegal to tap, or capture communications over wires[97]. This law was an updated form of the Federal Wiretap Act of 1968. Several subsequent legislations including the USA PATRIOT Act clarified and updated the ECPA to keep pace with the new technologies and methods.

Title I of the ECPA, which is referred to as the Wiretap Act, prohibits the intentional actual or attempted interception of any wire, oral or electronic communication. It also prohibits procuring any person to intercept the same[98]. It also prohibits the use of communications that are obtained illegally, as evidence[99]. Further, it provides certain exceptions to service providers and other people who are authorised to intercept wire, oral, or electronic communications.

Title II of the Act is referred to as the Stored Communications Act (SCA). It safeguards the privacy of the contents of the files stored by service providers. Secondly, it also protects the records of subscriber held by the service providers like subscriber name, IP address, etc.

Title III of the Act addresses pen register and trap and trace devices. It makes it mandatory for a government entity to obtain a court order authorising the installation and use of a pen register, a trap and trace device.

This law has not been very effective as it does not take into account how people currently share, store, and use information. Nowadays, people store data in clouds. In other words, it is quite outdated.

It is easy for government agency to demand service providers to give them consumer data stored on their servers. Emails that have been stored for over 180 days is considered to have been abandoned. The law enforcement agency can demand such

[96] Electronics Communication Privacy Act
[97] *Ibid*.
[98] *Ibid*.
[99] Electronics Communication Privacy Act.

emails but will have to justify that the information is relevant for an investigation. When the law was enacted, they did not have the current situation in mind, when emails are stored indefinitely as customers have access to nearly unlimited cloud storage.

FEDERAL LAWS

The federal government has also passed cybercrime laws such as:

CREDIT CARD FRAUD ACT – This Act is applicable when computers and other technologies are used to make fraudulent credit card transactions like duplicating card, gaining unauthorised access to card details, etc[100].

IDENTITY THEFT ASSUMPTION AND DETERRENCE ACT – This Act criminalised stealing others' personal data by posing oneself to be someone else in cyber space[101]. In other words, it prohibits data theft by impersonation.

ECONOMIC ESPIONAGE ACT – This Act deals with the theft of trade secrets and other forms of intellectual property[102].

CHILD PORNOGRAPHY PREVENTION ACT – This Act deals with criminalising the digital possession, production, and distribution of images or videos that show minors in sexually explicit conduct[103].

THE VIOLENCE AGAINST WOMEN REAUTHORISATION ACT This Act prohibits the use of computers or other electronic communication to harass, intimidate, threaten, kill or place one under surveillance[104].

FEDERAL CYBERSECURITY LAWS

Other Federal Laws which serve as cyber security laws are:

[100] Credit Card Fraud Act.
[101] Identity Theft Assumption and Deterrence Act.
[102] Economic Espionage Act.
[103] Child Pornography Prevention Act.
[104] The Violence Against Women Reauthorisation Act.

CYBERSECURITY INFORMATION SHARING ACT (CISA) The main objective of this Act is to improve cybersecurity in the US through information sharing about cybersecurity threats.

CYBERSECURITY ENHANCEMENT ACT OF 2014 – The purpose of this Act is to provide a public-private partnership to strengthen cybersecurity in the country.

FEDERAL EXCHANGE DATA BREACH NOTIFICATION ACT OF 2015 – This requires a health insurance exchange to update each individual whose personal information was unauthorisedly accesses due to security breach within a period of 60 days of the discovery of the breach.

NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015 – This law is an amendment to the Homeland Security Act of 2002. The main purpose of this Act was to enable the Department of Homeland Security's (DHS's) national cybersecurity and communication integration centre (NICC) to include the tribal governments and other private entities among its non-federal representatives.

Thus, the cyber laws and the cyber security laws and regulations of US have been continuously updated to keep pace with the technologies. It has been made stricter over time to equip organisations to secure the data from various cyber threats. However, cyber attacks on systems are still prevalent in US despite humongous efforts.

It is advisable that every entity becomes very active about securing their data. Cyber criminals are always on the hunt to attack computer systems. They are also continuously developing themselves in their approach to target the systems. Everyone should keep a regular check on their own systems to identify any kind of threat and address the loophole immediately.

CHAPTER VI

CONCLUSION AND SUGGESTION

CONCLUSION

Cybercrime is one of the fastest growing areas of crime across the world. Nowadays, more and more criminals are exploiting this branch of crime with the help of developing technologies. This type of crime includes attacking computer data and computer systems, identity thefts, distribution of child sexual abuse images and the like.

The global nature of cybercrime has enabled criminals sitting in one part of the world to attack a computer in another part of the world. This has necessitated all countries to adopt their own domestic laws to protect their own cyberspace. This is because the entire world is interconnected. With increased connectivity, there is also an increased risk of theft, fraud and abuse over internet. As we heavily rely on modern technology, we are becoming more vulnerable to cyber attacks. In simple words, cybercrime is the use of a computer as an instrument to further illegal ends. It basically involves a computer and a network. The computer may be used in the commission of the crime or target of the crime.

In India, the only legislation dealing with cybercrimes is the Information Technology Act. The Act does not provide any definition of the term 'cybercrime'. However, the scope of cybercrime has be made clear under the various provisions of the Act. The main purpose of this Act is to protect the field of e-commerce, e-governance, e-banking as well as provides penalties and punishments in the field of cybercrime. The Act has Been amended by the ITAA, 2008.

However, a single piece of legislation is not enough to protect a country with such a high rate of crime. Further, territorial jurisdiction is a major issue which has not been adequately addressed in the Act. Preservation of evidence is also big concern. However, most of the cybercrimes are also covered by the Indian Penal Code which is comforting factor for the investigating agencies. This is because criminals, even if

they are able to evade the IT Act, they will not be able to evade the provisions of the IPC.

US and UK also have a well developed legal system to address the issue of cybercrimes. India is developing day by day in every sector but in terms of cyber laws, it is behind the developed countries like US and UK. Most developed countries have separate rules, regulations and laws which deals with the cyber sector. However, in India, the Information Technology Act is not enough to deal with information technology and cyber sectors of India properly. India is making some progress to provide better services and protection in cyber sector. In 2013, the Government of India introduced a National Cyber Security Policy with the aim of protecting information infrastructure, reducing vulnerability, increasing capabilities and safeguarding it from cyber attacks. India should make the IT Act more efficient which needs some more amendments in the future. The difference in approach can be attributed to the different circumstances existing in these countries. There is a significant gap between India and the other two countries in terms of access to technology and resources.

Cybercrime is rampantly increasing across the world. One of the reasons for this is complex technology. Hackers are easily able to steal access codes, retina images, etc. to get past security systems. Secondly, storing data in small space makes it easy for people to steal data from other storage and use for their own profit. Thirdly, due to weak security control systems, attackers take advantage to commit crime. In terms of law enforcement, the major deterrent would be certainty of punishment which still does not exist in India. The conviction rate is still very low. Above all, the root cause of this is our heavy reliance on internet.

The IT Act does not cover all aspects of information technology that needs protection. Copyright and trademark violations have not been dealt with adequately in this Act. Even the internet service providers who transmits third party information have not been made liable under the Act. Thirdly, he Act does not specify how the extra territoriality will be enforced. However, apart from some gaps, the Act more or less covers all the major aspects of cybercrime.

To sum up, a crime free society is a Utopian concept. However, it should be the endeavor of all to keep the crime at the lowest. In a society which is heavily dependent on technology, crime based on electronic offences are definitely going to increase and law makers need to take extra measures to keep the fraudsters at bay. Technology, like all other things have good purpose as well as bad purpose. What is wrong is that when it falls in the wrong hands with a criminal intent who misuse them and then commit cybercrime. Hence, it should be the constant effort of the law makers to ensure that technology grows but is used legally and ethically and not for committing crimes.

FUTURE PROSPECTS

It is a known fact that cybercrime is not going to disappear altogether. Cybercrime is a side effect of our growing dependence on the internet. If something is useful, there will always be someone to misuse it. Cyber laws are all about mitigating the risks associated with the use of internet.

To deal with the risk, there needs to be a global legal framework along with adequate enforcement mechanisms. Many of the law enforcement agencies have developed expertise in dealing with hi-tech crimes. There must be an international legislation applicable globally without the limitation of any boundaries, development of 'cyber-interpol' to pursue criminals beyond geo-political borders. This way, we will progress in combating against cybercrime.

Law enforcement is not the only solution. We have to ensure that each individual and business entities are aware of the risks associated with the use of internet. All need to be aware of how to minimize their exposure to cybercrime. This is more important for inexperienced people who are regular users of online shopping, internet banking and social networking. It is highly essential to have mass public awareness programs about cybercrime and methods to mitigate the risks.

SUGGESTIONS

There is an urgent need for unification of laws relating to internet to reduce any kind of information. For example, for the offence of publication of harmful contents, we have IPC, IT Act, Data Protection Act, etc. all of which vaguely deal with the subject but lacks efficient enforcement mechanism. Due to many laws dealing with the same subject, there is always a confusion regarding their applicability and none of the laws deal with the subject specifically. Thus, there is a need for one cyber legislation.

One crucial problem in combating cybercrime is the inefficient enforcement mechanisms. Harsher laws are required to deal with criminals and also certainty of punishment is required.

Thirdly, it is very important to have Extradition Treaties among countries to make extra territorial provisions workable.

Lastly, all countries need to update their laws either by amendments or by adopting unified laws. There is a strong need to have better law enforcement mechanism to make the laws better workable.

.

TABLE OF STATUTE

India

- Information Technology Act,2000
- Indian Penal Code

UK

- Computer Misuse Act, 1990
- Serious Crime Act 2015
- The Police and Justice Act 2006

US

- Consumer Privacy Protection Act 2017
- Computer Fraud and Abuse Act 1984
- Electronics Communication Privacy Act 1986
- Credit Card Fraud Act
- Identity Theft Assumption and Deterrence Act
- Child Pornography Prevention Act
- Cybersecurity Information Sharing Act
- Cybersecurity Enhancement Act Of 2014
- Federal Exchange Data Breach Notification Act Of 2015
- National Cybersecurity Protection Advancement Act Of 2015

BIBLIOGRAPHY

Articles

- Aman Singh Bakshi, Bois Locker Room": The role of Intermediaries in regulation of content, published on Bar and Bench, 2020

- Darya Gudkova , Daria Bronnikova, 'Kaspersky Security Bulletin: Spam Evolution 2008', published on Securelist, March 2 , 2009.

- Dr Mohan Dewan "COVID 19 Lockdown: Increasing Cyber Crimes in India", Lexology 2020.

- Dustin Volz, "Yahoo says hackers stole data from 500 million accounts in 2014", Reuters , 2016.

- Harpreet Singh Dalla, Ms. Geeta, Cyber Crime – "A Threat to Persons, Property,Government and Societies", published in International Journal of Advanced Research in Computer Science and Software Engineering. 2013

- John Leyden, "How police busted UK's biggest cybercrime case", The Register, 2009.

- John Leyden, "Welsh virus writer Vallor jailed for two year", The Register, 2003.

- Kiratraj Sadana & Priya Adlakha, "Cyber Crime During Coronavirus Pandemic", Mondaq 2020.

- Mohak Rana, "Crimes in Cyberspace: Right to Privacy and Other Issues", publish on Lawoctopus, 2014

- Robert Roohparvar, "Elements of cyber security", InfoGuard Cyber Security, 2019.

- Shital Prakash Kharat, "Cyber Crime – A Threat to Persons, Property, Government And Societies" SSRN, 2016.

Books

- Anirudh Rastogi, "Cyber Law- Law of Information Technology and Internet*"*, 2nd ed., Published by Lexis Nexis, 2014.
- Dr.S.V.Joga Rao: "Law of Cyber Crimes and Information Technology Law", 2nd ., Wadhwa and Company, Nagpur, 2009,
- Farooq Ahmad, "Cyber Law in India (Law on Internet)", 4th ed., Allahabad Law Agency, 2011.
- Jyoti Ratan, "Cyber Laws & Information Technology", 3rd ed., Published by Bharat Law House, Delhi, 2017.
- M. Dasgupta, "Cyber Crime in India- A Comparative Study", published by Eastern Law House 2009.
- Talat Fatima, "Cybercrimes", 1st ed., published by Eastern Book Company 2011.
- Vakul Sharma, "Information Technology- Law & Practice", 5th ed., Published by Universal Law Publishing, 2016.

Websites

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/272311/6å875.pdf
- https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/
- https://www.computerevidence.co.uk/Cases/CMA.htm
- https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
- https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

- https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf
- https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654
- http://www.ijlp.in/ijlp/imageS/Volume%20-1,Issue-1(1),%20Mar-14.pdf
- https://privacyinternational.org/explainer-graphic/2273/understanding-difference-between-cyber-security-and-cyber-crime

Newspaper Articles

- India Today, available on https://www.indiatoday.in/crime/story/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1590345-2019-08-22, August 22, 2019
- Indian Express, https://indianexpress.com/article/cities/pune/malware-attack-cosmos-bank-gets-rs-5-72-cr-from-hong-kong-based-bank-6273134/, August 11, 2018
- Peter Victor, 'Black Baron a self taught whiz kid', The Independent, November 16, 1995.