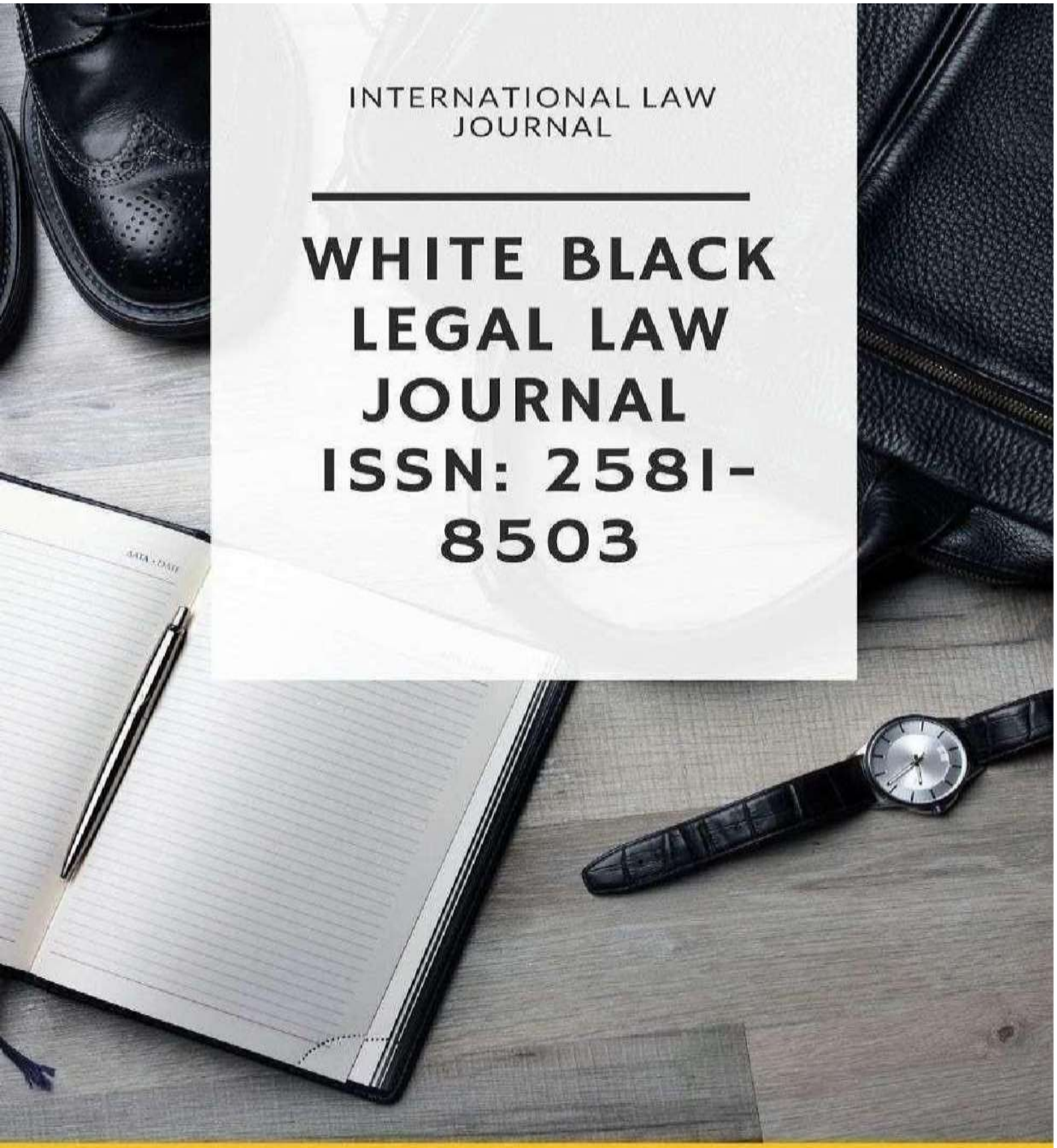

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

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

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

"A COMPARATIVE STUDY ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN STRENGTHENING CYBERSECURITY FRAMEWORKS: AN ANALYSIS OF INDIA, THE UNITED STATES, AND CHINA."

AUTHORED BY - NEHA SHARMA

Semester 10, Batch 2021-26

Dissertation submitted in partial fulfillment of the requirement for the award of the degree of

B.B.A. LL.B. (Hons.)

Submitted To

Mr. Manthan Sharma

(Lecturer of Law)

Unitedworld School of Law, Karnavati University

Uvarsad-Adalaj Road, Knowledge Village,

Gandhinagar, Gujarat, 382422

DECLARATION

I, Neha Sharma,20210401084, hereby declare that the dissertation on the topic: "A Comparative Study on the Role of Artificial Intelligence in Strengthening Cybersecurity Frameworks: An Analysis of India, the United States, and China" is my original work and has been carried out by me. I confirm that the content presented in this dissertation has not been previously submitted for the purpose of obtaining any other degree or diploma, to the best of my knowledge and belief.

Signature:

Name of the Student: Neha Sharma **Course:**

B.B.A-L.L. B (Hons.)

Date: (Date of Submission): 30/04/2026 Enrollment No.: 20210401084

Batch: 2021-26

CERTIFICATE

This is to certify that the research work entitled "A Comparative Study on the Role of Artificial Intelligence in Strengthening Cybersecurity Frameworks: An Analysis of India, the United States, and China" has been carried out by Mr. Neha Sharma,20210401084, under my guidance and supervision. This research work is submitted in partial fulfilment of the requirements for the B.B.A., LL.B. (Hons.) degree to be awarded by the Unitedworld School of Law, Karnavati University, Gandhinagar.

[Signature]

Name of the Supervisor/Mentor: Mr. Manthan Sharma

Designation: Lecturer of Law

Date & Place: 30/04/2026 (Gandhinagar).

ACKNOWLEDGEMENT

I would like to express my gratitude to several individuals whose support and guidance were invaluable in the completion of this dissertation. First and foremost, I extend my sincere thanks to Mr Manthan Sharma, Lecturer, Unitedworld School of Law, Karnavati University for his patience and faith in me and to help me to plan my dissertation and to provide insightful feedback and expert advice throughout every stage of this research. I am grateful for the opportunity to undertake this research work.

Neha Sharma

Contents

List of Cases

1. M.P. Sharma v. Satish Chandra → *M.P. Sharma Case*
2. Kharak Singh v. State of U.P. → *Kharak Singh Case*
3. Govind v. State of M.P. → *Govind Case*
4. R. Rajagopal v. State of T.N. → *Auto Shankar Case*
5. PUCL v. Union of India → *PUCL Case*
6. Maneka Gandhi v. Union of India → *Maneka Gandhi Case*
7. District Registrar v. Canara Bank → *Canara Bank Case*
8. Selvi v. State of Karnataka → *Selvi Case*
9. Shreya Singhal v. Union of India → *Shreya Singhal Case*
10. K.S. Puttaswamy v. Union of India → *Puttaswamy Case*
11. State of Maharashtra v. Madhukar Narayan → *Madhukar Narayan Case*
12. People's Union for Democratic Rights v. Union of India → *PUDR Case*
13. Romesh Thappar v. State of Madras → *Romesh Thappar Case*
14. Bennett Coleman v. Union of India → *Bennett Coleman Case*
15. A.K. Gopalan v. State of Madras → *A.K. Gopalan Case*
16. ADM Jabalpur v. Shivkant Shukla → *Habeas Corpus Case*
17. Naz Foundation v. Govt. of NCT Delhi → *Naz Foundation Case*
18. Navtej Singh Johar v. Union of India → *Navtej Johar Case*
19. Anuradha Bhasin v. Union of India → *Internet Shutdown Case*
20. Justice K.S. Puttaswamy (Aadhaar) v. Union of India → *Aadhaar Case*

Abbreviations

1. IT Act – Information Technology Act, 2000
2. SC – Supreme Court
3. HC – High Court
4. AIR – All India Reporter
5. SCC – Supreme Court Cases
6. Art. – Article
7. Sec. – Section
8. FIR – First Information Report
9. PIL – Public Interest Litigation
10. DPDP Act – Digital Personal Data Protection Act
11. UOI – Union of India
12. GOI – Government of India
13. NGO – Non-Governmental Organization
14. IT Rules – Information Technology Rules
15. CERT-In – Indian Computer Emergency Response Team

16. WWW – World Wide Web

17. VPN – Virtual Private Network

18. URL – Uniform Resource Locator

APTER-1

INTRODUCTION

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

- Carrie P. Snow

1.1 introduction

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

Information Technology has brought a drastic change in the human life. Human intelligence has advances the life as easy way of communication, commerce, business and the banking also. The progress of civilization, as evidenced by the ever-changing information technology, easily accessible by use of computers was, no doubt put to use for improvement in living standard of human being. Information technology made improvements in every aspect of human life as like education, industry, commerce, governance, personal life style and social life around the world.[1]

The information technology is very useful to the human life, which has madean impact on the social structure of the society. Especially the Indian culture is

quitedifferent but the information technology has connected the people. The social cites makes the platform to the nonprofessional to share their view, but along with the goodimpacts of it, certain adverse effect can be seen by the information technology.

[1] Information Technology Act, 2000 (India)

The privacy 1s going to violate by the cyber criminals, it create certain new mode to commit the existing crime, when the cyber space is going to be used for committing the crime.

Development changes the life style of human being but the human nature didnot change. Human ingenuity has also use the technology for committing technology. Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a *legal wrong that can be followed by criminal proceedings which may result into punishment."* The hallmark of criminality is that, it is breach of the criminal law. Asper Lord Atkin *"the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences" .*[2] A crime may said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime." *"Any criminal activity that* uses a *computer either* as *an instrumentality, target or* a *means for perpetuating further crimes* comes *within the ambit of cyber crime"*
Cyber crime is an evil having its origin in the growing dependence oncomputers in modern life. In a day and age when computers are running everything from microwave ovens and refrigerators to nuclear power plants, cyber crime has assumed rather sinister implications. The evil of cyber crime is product of the technology but the basic nature of human being is the same and one. Therefore, the technology is the easy way to perform the act, which is against the law. The term cyber space is new. However, it creates the new modes operands for committing the crime or an illegal act by using the means of computer.

The internet is a technical development gives us all opportunity to act as global community. Internet and electronic based treading affect all aspects of

---

[2] Indian Penal Code, 1860.

business. The information technology revolution is creating new business and forgoing old one to either change or die. The traditional legal systems have a great difficulty in keeping peace with the rapid growth of the internet and its impact throughout the world. Telephone (though invented by Bell) it gives easy way of communication, which is more effective than the conventional form of communication. An internet or network of computers can operate without the constraints of space, state borders etc.

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

Cyber crime is not different from the conventional crime. However, the tool has been changed so it requires different tools for investigation. The basic intention behind the cyber crime is nothing but wrongful gain or wrongful loss or it may result in defraud someone, which is the base of the conventional crime as like the theft andcriminal misappropriation or fraud. Therefore, the cyber crime is not different from the conventional crime and subject to the regular criminal law of lndia.[3]

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

need by the Indian legal system. The Indian Penal code cover all the crimes as contended the

---

[3] Information Technology (Amendment) Act, 2008 (India).

conventional crime, and for the execution of this law, effective investigation is required, and therefore the Criminal procedure code[4] deals with the investigation and powers to investigate. Execution of criminal law is much more depends on the effective investigation.

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

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

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

1.2 Aims And Objects:

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

situation of the society. Recently the amendment takes place in the Indian Penal Code in 2013, which drastically change the definition of the certain crime. Somewhere the provisions that

---

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

1s suitable to prevent the cnme, which is going to be committed by using the technology, such as the Indian Penal Code sec 354(0) which deals with the Stalking.

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

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

Following are the objective of research:

1. To observe the provision of Indian criminal law and the relevant provisions which cover the offences like cyber crimes.
2. To make the study of cyber law including I T Act and the relevant Penalprovisions pertaining to cyber crime.
3. To make the comparative study of conventional Criminal law of Indian and cyber crime and laws relating to cyber crime

To find out the shortcoming of the laws pertaining to cyber crime includingthe

procedural laws i.e. The Code of Criminal Procedure and Indian Evidence Act.

1.3 Significance of Topic of Research

Carrie P. Snow rightly said that the technology gives a wonderful gift to you by one hand and stop you by another hands. The present criminal law is in developedstage but the law behaves like a Hindu traditional wife, which 1s behind the seven steps from the technology. The technology developed in such a way that it now essential part of the life and therefore the present law is facing various challenges.

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

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

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

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

1.4 Literature Review:

Sr. No.	Nature of Literature	Name of Literature Covered / Review	Research Gap	Intended Research
1	Journal	**Taddeo, M., & Floridi, L. (2018).** ***How AI is Transforming Cybersecurity.*** **Journal of Cybersecurity.** Discusses global integration of AI into cyber defence through anomaly detection, predictive analysis, automated threat response, and digital ethics issues. Highlights AI' s potential to revolutionize cybersecurity by enabling real-time monitoring and rapid intervention.	• This article journal does not provide country-specific comparisons between India, the U.S., and China. • Lacks examination of how national policies affect AI-based cybersecurity adoption. • No analysis of geopolitical tensions shaping AI strategies.	• To compare AI-driven cybersecurity adoption across India, the U.S., and China. • To study the impact of policy, regulation, and governance on AI effectiveness.

2	Journal	**Borghesi, A. et al. (2020).** ***AI for Intrusion Detection Systems: A Global Review.*** **IEEE Security & Privacy.** Focuses on machine learning models used for detecting cyber intrusions globally. Highlights supervised and unsupervised models and their threat detection accuracy.	• This article journal has no study on national-level deployment in India, U.S., and China. • Does not examine differences in digital infrastructure maturity.	• To evaluate IDS adoption across the three nations and compare success rates.
3	Report	**US Department of Defense (2021).** ***AI and Cyber***	• Report focuses only on the U.S. and lacks	• To compare U.S. federal

Sr. No.	**Nature of Literature**	**Name of Literature Covered / Review**	**Research Gap**	**Intended Research**

		Defense Strategy. Provides detailed insights into U.S. federal initiatives to integrate AI into national	comparative global context. • No reference to developing countries like India.	cyber AI strategies with India' s an d China' s frameworks.
		cyber defense frameworks, military networks, and critical infrastructure protection.		
4	Report	**Indian Ministry of Electronics & IT (2020). *National AI Strategy and Cybersecurity Vision.* * Examines India' s AI roadmap, including proposed AI-based cyber threat monitoring and CERT-In operations.	• The report does not analyze India' s capabilities relative to major cyber powers like the U.S. or China. • Lacks discussion on budget, skill gaps, and AI readiness.	• To map India' s AI-cybersecurity preparedness against globa l benchmarks.

5	Journal	**Zeng, J., & Fang, E. (2019). *China's AI Security Architecture.* China Quarterly.** Explores China's AI-driven military cyber capabilities, digital surveillance, and national cyber defence strategy.	• In this article there is no comparison with democratic nations like India and the U.S. • Biased toward China's perspective without balanced evaluation.	• To provide a multi-country, comparative, and unbiased analysis.

Sr. No.	Nature of Literature	Name of Literature Covered / Review	Research Gap	Intended Research

6	Book Chapter	**Schneider, J. (2021). *AI and Geopolitics of Cybersecurity*. In Global Security Studies.** Explains how nations use AI to strengthen offensive and defensive cyber operations.	• This book chapter does not cover country-level case studies. • No analysis of regulatory differences affecting AI security adoption.	• To examine geopolitical and regulatory factors shaping cyber AI in three countries.

7	Journal	**Kshetri, N. (2020). *Cybersecurity in India: Challenges and AI Solutions.* Journal of Information Security.** Discusses cyber vulnerabilities in India and how AI can offer scalable monitoring solutions.	• This article focuses only on India. • Does not compare India's AI deployment with leading global cyber powers.	• To evaluate India's AI adoption relative to U.S. and China.
8	Journal	**Goodman, M. (2021). *AI Arms Race in Cybersecurity.* Journal of Strategic Security.** Highlights global competition in AI-based cyber warfare and strategic dominance.	• This article has no country-specific evaluation of AI readiness levels. • Lacks comparative metrics (funding, R&D, implementation).	• To compare investment patterns and AI R&D strengths across the three countries.
Sr. No.	**Nature of Literature**	**Name of Literature Covered / Review**	**Research Gap**	**Intended Research**

9	Journal	**Li, X. (2020).** ***AI and National Cyber Sovereignty in China.*** **Chinese Journal of Cyber Policy.** Explains how China integrates AI with cyber sovereignty and state surveillance systems.	• This article focuses heavily on governance surveillance; minimal discussion on general cybersecurity frameworks. • Does not compare with democratic cyber models.	• To contrast China's model with India' s and the U.S. ' s democratic AI frameworks.
10	Journal	**Smith, A. (2019).** ***AI-driven Threat Intelligence Systems.*** **Cybersecurity Review.** Examines global advancements in AI threat intelligence and predictive defence.	• This article is not tailored to national cybersecurity strategies. • No comparative dimension.	• To analyse national variations in AI-based threa tintelligence capabilities.

11	Report	FBI Cyber Division (2022). *AI-Augmented Cyber Defence Report.* Explores U.S. law enforcement' s adoption of AI for threat prediction, digital forensics, and malware analysis.	• In this report there is no cross-country comparison with India and China. • Focuses only on federal enforcement.	• To compare law enforcement-level AI adoption across the three countries.
12	Report	NITI Aayog (2021). *Responsible AI for India.*	• This report does not address India' s AI	• To examine India' s ethical

Sr. No.	**Nature of Literature**	**Name of Literature Covered / Review**	**Research Gap**	**Intended Research**
		Addresses ethical frameworks, responsible AI deployment, and cybersecurity implications.	cybersecurity gap compared to U.S. and China. • Lacks technical implementation details.	AI policies alongside foreign AI-cybersecurity models.

13	Journal	**Cheng, L. (2022). *AI-enabled Cyber Attacks and China' s Defence Strategy*. Security Studies.** Explores AI in China' s cyber offence-defence balance with emphasis on military cyber ops.	• This article is biased toward China' s state narrative. • Not compared to U.S. or Indian defence frameworks.	• To form a balanced comparison of cyber-offence readiness.
14	Journal	**Papernot, N. (2020). *Machine Learning Security*. IEEE Transactions on Security.** Discusses vulnerabilities in AI models such as adversarial attacks and data poisoning.	• This article focuses on technical vulnerabilities but not adoption differences in national strategies.	• To compare how each country addresses ML security challenges.
15	Journal	**Chaudhary, A. (2021). *AI and Cyber Policy in India*. Indian Journal of Public Policy.** Analyses cybersecurity policy	• This article have no comparative benchmarking with global superpowers.	• To positio n India' s AI strategy relative to U.S. and China.
Sr. No.	**Nature o f**	**Name of Literature Covered / Review**	**Research Gap**	**Intended Researc h**

	Literature			
		gaps and AI integration challenges in Indian infrastructure.		
16	Book	**Brundage et al. (2018).** ***The Malicious Use of AI.*** Covers global risks and cyber threats arising from malicious AI applications.	• In this book there is no comparison of mitigation approaches across nations.	• To explore country-specific AI threat response mechanisms.
17	Journal	**Hathaway, O. (2021).** ***International Cyber Law and AI.*** **Yale Journal of International Law.** Discusses legal frameworks governing cyber warfare and AI.	• In this paper there is no application to India, U.S., China-specific legal environments.	• To analyse legal frameworks influencing each country's AI strategy.

18	Journal	**Subramanian, R. (2022). *AI in India's Critical Infrastructure Security*. Journal of Digital Security.** Discusses AI integration in Indian energy + telecom network defence.	• This article is limited to Indian infrastructure; lacks global comparison.	• To benchmark India's critical infrastructure protection against U.S. and China.
19	Journal	**Green, T. (2020). *Automation and Cyber Defence in the U.S.* Cyber Tech Journal.** Explores deployment of robotics and machine learning in U.S. defence cybersecurity.	• This article is U.S.-centric; no comparative dimension.	• To compare U.S. automation with India's and China's cyber automation strategies.

Sr. No.	Nature of Literature	Name of Literature Covered / Review	Research Gap	Intended Research

20	Report	**OECD (2021). *AI and Global Cybersecurity Policy Review.*** Broad global assessment of AI policies and cyber frameworks across multiple nations.	• According to this report there is no in-depth analysis of India, U.S., and China specifically. • Lacks country-wise model comparison.	

1.5 Hypothesis:

Indian Criminal law is now well developed; so for as investigation of

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

Use of Internet to commit the crime Is punishable by the criminal law. Cyber crime is nothing but the subject of conventional criminal law but what development takes place regarding the Internet, which leads to cyber crime but the

criminal law hasnot amended in such a way that is why the problem of cyber crime is increase and need certain appropriate measures to curb it.

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

- Cyber crime is subject matter of the conventional criminal law.
- Cyber crime and conventional crime are not different but the way of committing the crime in cyber crime is different
- Cyber crime is expansion of the conventional crime, to control it certain new policies are required.
- There is close relation between cyber law and criminal law
- Cyber crimes more spread due to lacunas in the investigation process

New substantive laws are not required but procedural laws must be amended and expert investigation machinery and adjudicatory authority must be appoint for controlling the cyber crime.

To control cyber crime special investigation force must be need and the present investigation authority need the assistant of the expert in law and computer.

1.6 Research Methodology:

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

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

analyzing the Statute of Indian Legal System.

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

APTER-2

E LAW RELATING TO CYBER CRIME IN INDIA

The concept of crime Is not a modern one but it has been existing from time immemorial. However, time to time, the concept and nature of crimes have changed. In addition, the definition of crimes has been changed accordingly. In the era of 20th century and with the advent of computer, the criminals have changed the mode of committing the crimes from conventional methods to computer based methods. The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China.[5] Indian legal system is now in a developed stage. Indian Legal system is enacting the law along with the changing situation. As Prof. Allen has rightly contented that, the law is not only deals with command but is something more. This view shows that the role of law is broader than the command. This role of law is more relevant in the present situation. The criminal law closely connected with the each member of the society. In the age of information technology, cyber law is need of hours. The cyber law means the law relating to the cyber crime.

A person seating in any corner of the world can communicate to other personwithout disclosing his identity. Due to this nature of internet, it raised various challenges not only to the government but also to the trade and individual of the entire world. Therefore, the legal system awakens and required to make certain legislations to protect the interest of the entire society. Therefore, this new branch of law is emerged, because the conventional procedure to prevent the crime is useless for offences committed through the computer or internet. The rules and regulation, which deals with the cyber space internet and its regulation, are subject matter of the cyber laws.

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

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

2.1 Concept of Cyber crime

The term cyber crime Is nowhere defined, this concept Is vary because the crime which is going to committed by using any means of communication or internetcan be called as a cyber crime. The misuse of the computer or the internet is not specific therefore, it Is not possible to define the cyber crime specifically. To understand the concept of cyber crime, it is necessary to see the concept of crime, which is, attach with the computer and the internet. The concept of cyber crime is notradical different from the concept of conventional crime. Both include the conduct whether act or omission which causes breach of rules of law and counterbalance by the state[6].

In initial period, the crime is quite different and depends on the will of the sovereign authority. Now a days the crime is a social and political phenomenon and itis as old as the human society Along with the development, the concept of the crime is legal and back by sanction. Now crime means a legal wrong. Initially it is somewhere the religions wrong when the religious institutions were powerful. There were no difference between sin and crime. However, along with the development of State, the concept of sin was diluted and the sin or wrongful act term

in to a wrongfulact. This wrongful act now turns in to the concept of crime or offence. According to

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

Granville Williams, cnme or offence is a legal wrong that can be followed by criminal proceeding, which may result into punishment. The basic thing in criminality is that, it is a violation of criminal law.

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

In the present era of rapid growth, information technology is encompassing alllifestyles all over the world. These technological developments made the transition for paper to paperless transaction possible. We are now creating new standards of speed,efficiency and, accuracy in communication, which has become key tools for boostinginnovations, creativity and increasing overall productivity. Computers are extensively used in the storage of confidential data of political, social and economic or personal nature, which are of immense benefit to the society. The use of Computers is increasingly spreading, and more and more users are connecting to the internet. Due to this situation it is an easy access to the internet and the computer. Therefore, the criminals started to misuse the computer or internet for the criminal activates. The internet is a source where anybody can easily access, manipulate and destroy other information, this activities are nothing but the cyber cnme.

A generalized definition of cyber crime may be "unlawful act wherein the computer is either tool or target or both, the computer may be used as a tool in financial crime or sale of the any illegal articles. The computer may be the target when

someone tries to unauthorized access to the computer or any personal data; this kind of misuse of the computer or the computer networks is called cyber cnme.

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

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

2.1.1 Definitions

The cyber cnme 1s worldwide problem so various authority, national and international level tries to define the term cyber crime. Following are certain important definitions. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet. The Encyclopedia Britannica defines 'cyber crime' as anycrime that is

committed by means of special knowledge or expert use of computer technology. So what exactly Cyber Crime is. Cyber Crime could reasonably include awide variety of criminal offences and activities.

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

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

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

A computer crime defined by the U S department of Justice' s "As an illegal act requiring knowledge of computer Technology for its perpetration, investigation or prosecution" . However, the definition is not exhaustive as there are many acts, which can be called abusive activities concerning the computer but they are often not clearly illegal. Moreover, most of the cyber crimes are committed via internet but the definition has no reference to it.

Cyber crimes can be plainly define as " Crimes directed at a computer or computer system" But the complex nature of cyber crimes cannot be sufficiently expressed in such simple and limited term.7

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

This definition is also cannot cover the border aspect of the real nature of the Cyber crime, while defining the cyber crime, it only cover the illegal activities pertaining

---

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

to the data transmission. However, the cyber crime not only deals with the data transmission, it includes every illegal activity via computer.

In 2001, The Council of Europe Convention defines cybercrime in Articles 2-10 in four different categories: 1) offences against the confidentiality, integrity and availability of computer data and systems; 2) computer- related offences; 3) content-related offence; 4) offences related to infringements of copyright and related rights.[8]

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

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

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

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

the cyber space to commit, any illegal act that can be called as a cyber crime.

---

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

The information Technology bill, 1999 defines the cyber crime as, "Whoever knowingly or intentionally council, destroy, or alter or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document use for a computer, computer program, computer system, or computer network, when computer source code is require to be kept or maintain by law the time being in force shall be punishable with a fine which may extent up to rupees two lakhs or with imprisonmentup to three years, or with both." [9]

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

- A criminal activity that involve unlawful access to or utilization of computer system.
- Any illegal action in which a computer is use as a tool or object of a crime; in other words, any crime, the means or purpose of which is to influence the functions of a computer
- Any incidents associated with computer technology in which a victim sufferedor could have suffered loss and a perpetrator, by intention made or could have made a gain.
- Any violation of the law in which computer is a target of or the means for committing crime.

Any activity, which involves the unauthorized and unlawful access to or utilization of computer system or network in order to tamper with the help of computers and the internet, can broadly be called as cyber crime.

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

merely a computer. Therefore, the mere computer or the internet is not subject of thecyber crime, but both things are part of the cyber crime. Therefore it is difficult to define the cyber crime .Basic reason behind it is

that, it is not

---

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

different that the conventional crime and it cannot be subject to any particular way of misusing of computer or the internet.

2.1.2 Essentials of Cyber crime:

The term cyber crime cannot define due to the critical nature of it, because it involves the crime relating to computer and computer techniques. [36] Therefore, it has not any specific ingredients different from conventional crime apart from the techniques. Because development of technology create new way to commit the crime called the cyber crime has emerged which is radically different from the conventional crime. This crime is the ill effect of the development of internet regime. In view of the peculiar nature and repercussions of cyber crime, its characteristics are altogether different from that of a conventional crime. The most striking features of cyber crimes are that they are relatively easy to commit, difficult to detect and even harder to proved. This is the reason as to why these crimes have been characterize as low risk high rewarding ventures for the cyber criminals who with basic computer knowledgeand skill can easily destroy valuable database causing huge loss or damage to the affected victims of the crime.[10]

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

with the routine working system and has a good understanding of the loopholes and availability of opportunities to commit the cyber crime without leaving any trace for possible detection. Apart from the employees who are unhappy with their employees for one reason or the other may tend to target the employees computer system to take revenge similarly, business rivals may also try to have unauthorized access to system of their computing counterpart and steal away confidential secret data from his computer system for personal gain. [11]

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

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

Cyber crimes have been characterized as high tech offences because they are committed by the abuse of computer networks and telecommunication technology. The range of such crime is wide enough to affect the socio-economic and the legal rights of the people. Through, the use of computer network system in itself is legal but the illegal actions in using the networks as a medium are deemed illegal andpunishable under the criminal law or the cyber law or both. Like any other cyber crime the hi-tech cyber crime committed through the computer telecommunication networks has the following

- The perpetrators as well as the victim both remain anonymous and difficult to be identified.
- Many unspecified potential customers are used through they may be far away from the place of crime.

Evidence against the crime is easy to erase thus rendering the helpless.

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

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

The United Nation highlighted the problem of definition in its manual on the

prevention and control of computer- related crime, stating that although there is consensus among experts, these definitions have been functional and hence too specific. A similar problem was expressed by the Council of Europe, the committee

on crime problem decided to leave out any definition of high tech crime in the Convention on Cyber (2001), allowing individual jurisdiction to apply their own definition based on their specific body of law. It is however interesting to note that the IT Act 2000 too omits to define cyber crime or computer crime. This Indian situation, though the Indian legal system enacted cyber law very recently in year 2000. Even themajor cyber laws of the US and UK do not content a definition of cyber crime. However, the taxonomy of these elusive crimes would give a circumvention and exhaustive comprehension of cyber crime. In India, the recent amendment in the IT Act, 2008 has used the term' "computer related offences" whereby a good number of cyber crime have been added to the list of crimes already existing.

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

1.2.3 Reasons for Cybercrime

Crime is a social phenomenon and there are various reason behind the crime. Criminologist had studied by giving different reason but the entire criminologist gives different reason. Cyber crime is creation of the technology and the technology makes the life of human being easy, therefore every one attracted towards this technology without sufficient knowledge. This technology is having various special feature due to which is gives opportunity to the misuse the technology for commission of crime. As Prof. H. L .A. Hart in his classic work entitled, "The concept of law" [12] has stated that, human beings are valuable to unlawful acts which are crimes and therefore, rules of law are required to protect them against such acts. Applying the same analogy to cyber space, the computer systems

despite being hi-tech devices are extremely vulnerable Computer is an electronic device which carries out its functions with the help of complex technology rather than manual actions of human beings. The greatest

---

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

advantage of networking in the computer age is the wider access to information resources over a large and extensive medium More and more organizations are restoring to networks for providing easily accessible information to their employees customers and parties with which they deal.

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

Wider access to information

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

Complexity of computer system

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

Negligence of Network users

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

Non- availability or loss of evidence

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

The inadequacy of traditional methods of evidence and crime investigation has necessities adoption of new techno-legal procedure called cyber forensics, which hasbroadly been classified as computer forensics and network forensics. The forensic experts play an important role in collecting and presenting admissible

evidence electronic evidence, search and seizure of material evidence relevant to the cyber crime under investigation. But still these are certain grey areas which enable the cybercriminals to tamper with the evidence to mislead the investigating agencies.

Jurisdictional Uncertainty[13]

Cyber crimes cut across territorial borders which undermine the feasibility and legitimacy of applying domestic laws which are normally based on geographical or territorial jurisdiction, Cyber crimes are committed through cyberspace network inter connectivity and therefore, they do not recognize geographical limitations because of their transnational in nature. There being no uniformity in law and procedure among the different nations for handling cyber criminals, jurisdictional conflict a serious problem for a nation to deal with the cyber offenders. In many cases, it so happens that create particular cyber activity is recognize as a crime in one country but it is not so in the other country where the criminal or the victim resides with the result the criminal easily escapes from prosecution.

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

2.1.4 Types of Cyber Crime:

The cyber crime is generic term that can be use by various illegal activates where in computer or computer network is going to use. The computer crime and cyber crime are literally different but that cannot separate from each other by the legal system. Therefore, it is not easy to classify the cyber crime. There are various modes and manner by with the cyber crime can be committed. Even the

traditional crime is going to be committed by using the computer or internet.

The concept of crime is

---

[13] Conventional crime through computer e-book.

itself dynamic, and in case of cyber cnme, it is more dynamic. Therefore, the cyber crime can be classified in various ways. It may classify on the use of computer or mode of using of computer in any crime. The role of computer in every cyber crime is different so it can classify on that basis also, it can classify on the basis of perpetrator. Role of computer means insider and outsider. However, the mode or role is not subject matter of criminal law but the result is more important, therefore on the basis of result of illegal act, Thus the cyber crime can be classified on the basis of victims in the manner as following

1. Crime affecting Individual
2. Crime affecting economy
3. Crime affecting national security

1. *Crime affecting Individual*

Cyber crime has started to take place by this kind. Maximum cyber crimes arecommit which affect the individual. In this cyber crime, the victim is the user of the computer or someone used the computer by the name of the victim. The criminal get access to the computer or account of the other and uses the private access by violatingthe privacy right of the victim. The computer is a common and important source of preserving personal data or information. Internet and the computer develop the techniques to restore the huge data of person in minimum time. Due to the capacity and the easy manner, this techniques is going to use in everywhere from school to hospital and business enterprises to governmental and nongovernmental banking alsomake use or abuse of it[14].

Internet and computer in business is call e-commerce. This e-commerce provides various speedy and less expensive procedures in the high- tech business. Thus e-commerce has removed the national boundaries without any problem. Due to

this, less

---

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

expensive process attracted the traders and businessperson to use this mode for transferring the huge amount of money. However, this process is also not without disadvantages.

The businessman and common man uses this technology to save their time, but criminals use the technology which is unknown to the general user of the internetand the technology is more sophisticated technology which is more easier way to commit the criminal activities. The criminal activity as like hacking and IP spoofingare the common offence, which are going to commit against the economy. Generally, the frauds are going to be committed by using internet. Software piracy is the common offence in a day, the object behind software piracy is nothing but to save themoney. Cyber squatting is another mode to commit the cyber crime. The main objectbehind these offences is nothing but to gain wrongfully. This is new mode to commit conventional crime though, it is known as a cyber crime.

2. ***Crime affecting National Security:***

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

This mode of the cyber crime threats the national and international perspective. Cyber terrorism is best example of this offence. Terrorists are using the recent information technology to formulate the plans, raise funds, create propaganda, and to communicate massage among themselves to execute a plan. [15] Cyber warfare is another mode to commit the cyber crime which affect the national security. Computer and internet is integral part of military strategies of various countries in the

world. By using the technology when one country collects the information of enemy country, it creates

---

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

the threat to that country as well as the peace and security of the world 1s going to be affected by this kind of activities.

The cyber crime is generic term that can be use by various illegal activates where

in computer or computer network is going to use. The computer crime and cyber crime are literally different but that cannot separate from each other by the legal system. Therefore, it is not easy to classify the cyber crime. There are various modes and manner by with the cyber crime can be committed. Even the traditional crime is going to be committed by using the computer or internet. The concept of crime is itself dynamic, and in case of cyber crime, it 1s more dynamic. Therefore, the cyber crime can be classified in various ways. It may classify on the use of computer or mode of using of computer in any crime. The role of computer in every cyber crime isdifferent so it can classify on that basis also, it can classify on the basis.

2.1.5 Cyber Crime and Offences under Indian Penal Code

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

Indian legal system enacted Information Technology Act, 2000 with intent toregulate the e-business. That is purely a contractual law dealing with the commerce, but along with e-business, it provides certain provisions dealing with unauthorized use of the internet or unauthorized use of the computer. This

misuse is called as a cyber crime in The Information Technology Act, 2000, which is India' s cyber Law. The offences provided in this Act are already provided in Indian Penal Code in the variousprovision from the enactment of the Indian Penal Code.

After coming into force of the Information Technology Act, 2000 on 17th October,2000 appropriate provisions have been incorporated in the substantive criminal law of India. The substantive criminal Law of India means Indian Penal Code, because the various offences of this law are too much similar to the offences which are known cyber crime, only due to technology to commit that offences is quite different therefore the amendments are require to bring that offences under the preview of this Code. The amendment insert certain new term in the Indian Penal Code only with intent to make effective implementation of provisions dealing with this offences which are going to commit by using the information technology.

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

Similar offences also fall under the BNS 2023.

1. Sending threatening messages by email Section 351 (1) BNS
2. Sending defamatory messages by email Section 356(1)BNS
3. Forgery of electronic records Section 336 (1) BNS
4. Bogus websites, cyber frauds Section 318 BNS
5. Email spoofing Section 336 BNS
6. Web-jacking Section 308 BNS
7. E-Mail Abuse Section 356(2) BNS
8. Online sale of Drugs NDPS Act
9. Online sale of Arms Arms Act
10. Pornographic Section 294 BNS

2.2 Cyber Crime and Criminal law of India:

Cyber crime is undefined concept, which means the criminal activity done byusing the computer and internet. Cyber crime is a boundary less crime. Until the 1999, Indian

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

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

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

The Indian legal system has enacted Information Technology Act in the year

2000. The said act is mostly deals with the e-business and the regulation of e-commerce. Along with this, it recognized certain cyber crime. However, the Information

Technology Act is enacted, Which deals with the regulation of digital signature and the authorities regarding it, The I.T. Act does not provide completely about the cyber crime but the other criminal law also deals with the cyber crime. Indian Penal code also deals with the certain computer crime because cyber crime isnew mode of the committing crime, which is not so much different from the conventional crime. However the cyber crime is committed by using the different modus operandi, therefore some amendments are require to cover the technical aspect. Therefore, the cyber law is enacted by the legal system. India is one of the countries among them, which are having alertness regarding the crimes going to be committed in cyberspace.

2.3 Evolution of law in Cyber Space:

The modern world is of the cyber space, 21st century gives us a new world of internet. It drastically changes the life style of human being. Internet is now a lifeline in the present days. One or other way now connects everyone with computer. Every person generally using cell phone, laptop, tab computer etc. Computer takes place of paper and all records, so that personal data is now on computer or in the cyber space.So for protecting the personal information and data in the cyber space the laws are required. Cyber space represents the medium of communication, electronic. An internet or network of computers can operate without the constraints of space, state borders etc. Though they are only a medium for storage, analysis and communication of information, communication that is fast outmoding or even replacing more traditional method of communication. Therefore, cyber laws are the requirement and need of time. The convergence of the computer network and telecommunication facilitated by digital technologies has given birth to a common space called cyberspace. The new shorter Oxford Dictionary explains the expression Cyberspace as, "the national environment within which electronic communication occurs, especially when represented as the inside of the computer system." [16]Space

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

perceived as such by an observe but generated by a computer system and having no real existence, the space of virtual reality.

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

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

The main functions of the internet have thus emerged as providing

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

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

2.4 Indian Law on cyber crime

India also, like other countries of western has a well-developed legal infrastructure and it is going with the development and time. The result of this, India too is sharing the legal liability, which is the outcome of the

technological boom. Though the India 1s having rich heritage of the legal system, then also it facing the problem

of the traditional notion of the jurisdiction which is the great difficulty for the laws related to the cyber space.

India has emerged as a world' s leader in the field of Information technology ,because the earning from the software and the IT services is nicely contributing the Indian economy. With increasing in the growth and development of information technology and cyber world, the possibility of increase in the crime relating to computers has also increased simultaneously. Legislative steps for regulating the electronic commerce and checking the cyber crimes have also become essential. The Indian Parliament therefore enacted the Information Technology Act, 2000. For combating crime problem The Indian response in the form of legislative action as wellas the IT revolution is mainly limited to this Act and Rules and Regulation made thereunder.[17]

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

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

1. ***Information Technology Act:***

To regulate the electronic communication the Indian Parliament has enacted this Act, which involve the use of alternatives to the paper base means of communication and storage of information, to facilitate the electronic filing with thegovernment

agencies. Along with the enactment of the IT Act 2000, to recognize the electronic communication certain important amendments has made in the Indian laws, the amendments are required to make the execution of the regular laws in the

---

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

information technology age. The main object of the IT Act is to facilitate legal reorganization and regulation of commercial activities through electronic medium. This Indian Act is based mainly on the United Nations resolution No A/GES/51/162; Dated 30th January, 1997, as well as on the UNICITRAL Model Law on Electronic Commerce.[18] This is only one act in Indian legal system, which known as the Cyber Law of India.

A. As K.P. Singh has rightly pointed out the major issue covered under the provision of the act are as following[19].

B. Establish rules which recognize and validate contracts and execution through electronic mediums;

Recognizes the admission of computer evidence in courts and arbitration proceedings

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

2. Nature of the I.T. Act, 2000:

It is well recognized that it Is mainly enacted to recognized and facilitate e-commerce and not to govern cyber crimes, however the Act defines certain offences and penalties. Chapter XI of the act deals with offences and the Chapter IX deals with penalties and the authorities regarding adjudication. These two

chapters of the I.T. act

---

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

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

deals with certain cyber crimes. Chapter IX focus on the following important features:

A. Regulating conduct in its unique way;
B. Civil regulations to be employed by premise rather than criminal;
C. The process of adjudication 1s entrusted to adjudicating officers rather than regular civil courts;
D. Such adjudicating officers are required to know the laws and the IT or must have judicial experience;
E. Adjudicating officers are vested with power of civil court;
F. The proceeding to be conducted by such adjudicating officers are to be construed as judicial proceedings;
G. The quantum of compensation to be calculated at market rate for loss or sufferings.

This features shows that this chapter mere g1ves of civil court, certain provisions deals with power to impose the penalty. When these provisions of IT Actwhich deals with the civil liability, and if the act is comes under any penal provisionof Criminal law, then it can registered under that Laws also.

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

Section 65: Tampering with Computer Source Document: Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowinglycauses another to conceal, destroy or alter any computer sources code use for a computer with fine which may be extendedup to two lakh rupees or both .[20]

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

of thecomputers accession. For this, the punishment is provided up to the three years. Thissection essentially tries to stop the efforts or actions or commands given to the

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

computer to alter the programs, destroy the programs or to cancel them in such a waythat they cannot be used by the person who owns the program. Whether this is intentional or mischievous act but it attracts the punishment up to three years or fine up to two lakhs rupees.

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

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

Section 66 deals with the offence of unauthorized access to the computer resource. In the language of the computer, it is called hacking. The act in this offence is going to be committed by using the dishonest intention. [21]

- Information Technology (Certifying Authorities) Rules, 2000
- Information Technology (Security Procedure) Rules, 2004
- Information Technology (Certifying Authority) Regulations, 2001

As the said act also cannot fulfill the need of the time and the cyber security isfacing the problem as well as the execution is impossible due to certain technical problem.

---

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

Therefore, the Information Technology Act is drastically amended in the year 2008. The said amendment has made to bring the cyber crime under the preview of the conventional law.

3. The Information Technology (Amendment) Act, 2008

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

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

4. New cybercrime under I T Amendment Act, 2008:

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

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

For other offences mentioned in Section 66, punishment prescribed is generally up to three years and fine of one/two lakhs has been prescribed and these offences are cognizable and bailable. This will not prove to play a deterrent factor for cyber criminals.

Further, as per new Section 848, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and thenew Section 84C makes attempt to commit an offence also a punishable offence with imprisonment for a term, which may extend to one-half of the longest term of imprisonment provided for that offence.

In certain offences, such as hacking (sec 66) punishment is enhanced from three years of imprisonment and fine of two lakhs to fine of five lakhs. In Section 67, for publishing of obscene information imprisonment term has been reduced from fiveyears to three years (and five years for subsequent offence instead of earlier ten years) and fine has been increased from one lakh to five lakhs (rupees ten lakhs on subsequent conviction). Section 67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that

may extend to five years with fine up to ten lakhs. This prov1s1on was essential to curb MMS attacks and video voyeurism. Section 678 punishes offence of child pornography, child' s

sexually explicit act or conduct with imprisonment on first conviction for a term up to five years and fine up to ten lakhs. This is a positive change as it makes even browsing and collecting of child pornography a punishable offence.

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

Thus, the important changes takes place 1n I.T. Act 2008, which brings the various crimes, which are committed by using the computer or any communication device. Then also various cyber crimes are going to be registered using the Indian Penal Code. It shows that the Amendment cannot cover all the cyber crimes, becausethe cyber crime is basically different from the conventional crime, however the way to commit the crime is changed and the computer is a tool to commit the crime or in certain crime it is target.[22]

5. Indian Penal Code .1860

Indian Penal code is the universal criminal law of India. The base to constitute the offence is nothing but the guilty intention and prohibited act according to the Indian Penal code. The Indian penal code is basic criminal law of India, along with the time, the legal system enacted certain special criminal law. The cyber crime is creation of information technology age, though the modes or ways to commits cyber crime is different from the conventional crime, but it is not much

different from the conventional crime. The IT Act has not covered all the cyber crimes; again, Indian

---

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

Penal code is applicable. Due to the universal nature of the BNS , it covers almost all the crime.

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

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

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

Fraud on the internet is big business. Most of the cyber crimes comes in the category of fraud, but the Information Technology Act has not define the concept of fraud therefore most of the offences comes under the preview of the Indian Penal

Code. Section 2(9) BNS definitions fraudulently as a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise. The IT ActSection 668 used the word "dishonest intention" which is not defined in the IT Act then one can refer to BNS , which is a general legislation in the area of criminal law.

When any cyber fraud is committed in real sense it would be cheating which isdefined in section 415 of BNS . when any person makes the cheating by using internet it is very easy to him to hide his identity, this act perfectly comes it the offence provided under section 416 of BNS . that is cheating by personation. Apart from this various cyber offences are relevant under the sections as like 405,406,463,465 of BNS

. even the launching of virus Is provided under section 43 of LT.ACT is comes under the preview of sec. 425 of BNS . The act of launching of virus and other computer contaminants, would also amount to criminal offence of mischief. If the essentials of mischief are satisfied it would be an offence too.

Thus, the Indian Penal Code almost covers various cyber crimes, but considering the needs and development along with the information Technology Act certain important amendments made in Indian Penal Code in 2000. The amendments are sought to bring the paperless transactions under the preview of conventional criminal law. This amendment is suitable in the age of electronic commerce. Due to amendment the Act eliminated the basic requirement of paperless record and documents because substantive as well as procedural law, Indian Penal code, 1860, Indian Evidence Act, 1872 and even Criminal Procedure Code.

In Indian Penal Code the certain words as like 'computer resources' or 'electronic record' are inserted in various sections as like section 119,167,173,175 etc.

Thus, the Indian Penal Code covers the cyber crime. Even the Criminal Law Amendment Act 2013 has inserted certain sections, which are covering the offences which are going to be committed by using the computer or any

communication device. Section 354 C deals with voyeurism and Section 354 stalking, these offencesare subjected to the internet and communication device. Therefore the cyber crime though new kind of

offences are subjected to the Indian Penal code. If we see the Section 354D. it is as following

Sec. 354D. Stalking - {1) Any man who-

I. Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

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

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

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

II. It was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

III. In the particular circumstances such conduct was reasonable and justified.

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

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

6. ***Cyber crimes in Indian Penal Code***

1. Cyber Stalking

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

2. Cyber squatting

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

3. Data Diddling

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

4. Cyber Defamation

Cyber defamation is not too much different than the defamation provided in Sec.499 of BNS .it is nothing but any derogatory statement, which designed to injure a person·s business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers or the Internet, as like, someone publishes

defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

5. Trojan Attack

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

6. Forgery

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

7. Financial crimes

This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both SNS and IT Act. Therefore when suck crimes takesplace, both laws can be attracted. A leading Bank in India was cheated to the extentof 1.39 corers due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

8. Internet time theft

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

9. Virus/worm attack

Virus is a program that attaches it selves to a computer or a file and then circulates to other files and to other computers on a network. They usually affect thedata on a computer, either by altering or by deleting it. Worms, unlike viruses do notneed the host to attach themselves They merely make functional copies of themselvesand

do this repeatedly until they eat up all the available space on a computer's memory. This is one kind of trespass in the conventional crime. Though it is purely acyber crime, It covers under the Indian Penal code.

10. E-mail spoofing

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

Email bombing

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

11. Salami attack

This is basically related to finance and therefore the main victims of this crimeare the financial institutions. This attack has a unique quality that the alteration is so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program whereby a meager sum of Rs 3 is deducted from customers account. Such a small amount will not be noticeable at all.

However, due

such merger from all the account holders collect huge amount. This 1s purely acriminal breach of contract.

12. Web Jacking

This term has taken from the word hijacking. Once a website 1s web jacked

theowner of the site looses all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site. As it is one kind of hacking, but the IT Act has not use the word hacking specially, but

deals with the various kind of unauthorized access or tampering with the computer resources, IT Act cannot cover all kind of hacking therefore BNS is generally applicable to such kind of the unauthorized access.

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

7. *Indian Evidence Act and Criminal procedure Code*

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

3 relating to interpretation clause words [1]Digital Signature· and [1]Digital Signature Certificate·, the words [1]Electronic Signature· and [1]Electronic Signature Certificate· are substituted.

In Criminal Procedure Code, after Section 198 A[23], Section 198 B has been inserted according to which, [11]No Court shall take cognizance of an offence punishable under Sections 417, 419 and 502 of the Indian Penal Code, except upon acomplaint made by the person aggrieved by the offence[11]. Moreover in the Indian Penal Code the meaning of some words like [11]offences[11] and [11]computer resource[11] has

been made more exhaustive which take colour from the IT Act, 2000. It shows that India is successful in facing new challenges of IT. Many amendments have been made in the Copy Right Act on the argument that certain knowledge

should be treated as

---

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

private property and capable of 'Ownership'. Considering the requirement of society now, cyber law is providing a worth in administration of justice.

Cyber laws in India.

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

Common Law (governed by general principles of law)

- The Bankers' Book Evidence Act, 1891
- The Reserve Bank of India Act, 1934
- The Information Technology (Amendment) Act, 2008 and 2009
- The Information Technology (Removal of difficulties) Order, 2002
- The Information Technology (Certifying Authorities Rules, 2000)
- The Information Technology (Certifying Authorities) Regulations, 2001
- The Information Technology (Securities Procedure) Rules, 2004

Various laws relating to IPRs.

Thus, the Indian legal system Is having various laws concerning the cyber crimes. But the nature of the cyber crime is technical, therefore it require the technicalprocess to execute the criminal law in proper sense. The technical process is lackingin Indian legal system, therefore though the substantive criminal law is sufficient, but due to lacking in procedural aspect its unable to execute it in India. The basic problem in the cyber crime is that, there is specific manner by which the internet can be misuse; it is on the criminals, that they always misuse

it in different manner, therefore

it is not possible to the legal system to meet with the need. Apart from this, the nature of cyber crime is transnational, therefore it required the international co-operation. Mere making laws is not sufficient, cyber law cannot work without the international co-operation. The Information Technology Act 2000 and all the related laws having provision regarding the transnational jurisdiction, but execution is possible when all countries in the world recognized that act as a crime, and allow the proceeding on thataspect.

CHAPTER - 3

JUDICIAL RESPONSES: RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION IN INDIA

Use of computer, internet and information technology facilitate the personal and business transactions at person's own convenience. For use of technology, submitting personal information is a precondition. By each access, the personal information is deposited and gathered in large quantity with the entity which provides service. It is expected that this information shall remain confidential and private. Threat to personal information has increased due to globalisation and privacy of person is endangered. This threat is not limited to physical harm due to cyber-crimes but affecting the liberty and freedom to make choices due to excessive marketing. Even the information collected by government for provision of services, privacy and confidentiality of it may also be threatened.

By enacting different legislations, legal systems tried to control and regulate transactions done using information technology. The major challenge before any legal system is to balance the rights of the persons and interests of the state. In India after 1990, due to globalisation, use of computers and internet had increased. To protect the business interests, and e-commerce transactions, The Information Technology Act, 2000 was enacted. To make it more strong, provisions controlling cyber-crimes were added after its amendment in 2008. But for the protection of the information which is deposited and gathered with the body corporates-entities which provide services- its control and regulation under it is inadequate.

In the days of absence of legislative control mechanism i.e. from the beginning of 20th Century, the protection to privacy was provided by courts. Courts have provided protection against the state actions threatening physical, proprietary privacy. They also provided protection against the informational privacy invaded by state as well as

private entities as innovative uses of advanced technology harming it. This protection was

granted by interpreting the existing laws including provisions for fundamental rights under Constitutional law.

Illustrating the Court' s function while controlling the invasion, Supreme Court held in Canara Bank[24] that "Intrusion into privacy may be by a) legislative provisions,

b) administrative/executive orders and c) judicial orders. The legislative intrusion must be tested on the basis of reasonableness as guaranteed by the Constitution and for that purpose court can verify the proportionality of intrusion i.e. the purpose sought to be achieved. Administrative or executive action is concerned, it is to be reasonable and this reasonableness is verified from facts and circumstances of the case. As for the judicial action, e.g. intrusion may be through issuance of warrant, the court must have sufficient reason to believe that the action is necessary to uphold state interest. For this extent of the action shall be prescribed which only protect the state interest and not encroach the rights of the person unnecessarily. The order of the Court must observe that the action will be taken in good faith, intended to preserve evidence, or intended to prevent sudden danger to person or property" [25].

The researcher has discussed the judicial decisions for the protection of Right to Privacy and data protection in different countries including India in the following paragraphs.

3.1 Judicial decisions on Right to Privacy and Data Protection in India

Though before independence, some decisions were given by the Supreme Court of undivided India, in which the Right to Privacy was upheld. In India, the vacuum of absence of common law provisions for protection of privacy is filled with the judicial activism of Supreme Court. The Supreme Court of India has come to rescue of common citizen by construing 'Right to Privacy' as a part of fundamental right to life and personal liberty under Art. 21 of Constitution of India.

24 District Registrar and Collector, Hyderabad v. Canara Bank, (2005) 1 SCC 496

25 District Registrar and Collector, Hyderabad v. Canara Bank, (2008) 1 SCC 496

As in other judicial systems, the right was associated with enjoyment of property in India, may it be house or land. As India was ruled by England, we can see the development from the 19th Century. The courts in British-India upheld the right in different cases. These decisions were given by British India Courts and the Judges of Sardar Diwani Adalats.

3.2 Before Independence

The protection of right to privacy had appeared in the reports of British India courts for the first time after 1850. In 1855, in the decision of North-Western Province in Nuth Mull (1855)[26], the question of privacy arose. In this case Begbie, Smith and Jackson JJ held on appeal from the decree of the principal Sadr Amin of Delhi, that the erecting by the defendant of a new house, so that the plaintiff's premises were overlooked from the roof of the new house and their privacy thereby interfered with, gave the plaintiff a cause of action against the defendants.

Reports of some of the decisions are found in other decided cases after those cases. As this case of Nuth Mull was referred by Chief Justice Edge in **Gokal Prasad (1888)**[27], where the court observed that due to destruction of records during mutiny of 1857, it is not possible to ascertain whether there was a custom of privacy in this part of India. It was never proved or called in question prior to 1855 and owing to same cause and to absence from the report of the case on Nuth Mull and Kureem Oolah Beg of information on the point it is not possible to ascertain whether the judges of Sadr Diwani Adalat of North-Western Provinces were following the law as it was found existing or decided the case from the facts found.

In the same way, in case of Gokal Prasad, C.J. Edge referred to a number of cases on privacy. They were, Gunga Prasad (1862)[28], where Ross and Roberts, JJ. did not suggest any doubt that a right to privacy could exist, in Banaras case of Goor Das(1867)6- and

26 Nuth Mull v/s Zuka-Oolah Beg Sr.D.A.N.W.P.R.1855

27 Gokal Prasad v.Radho ILR Allahabad (10), 358 (1888),

28 Gunga Prasad v. Salik Prasad S.D.A.N.W.P. Rep. 1862 Vol. II, 217

also in Moradabad case of Ram Baksh (1867)[29], Morgan C.J. and Spankie J. expressly recognised the existence of a right to privacy. In 1886, Mata Prasad v. Behari Lal,8 Straight and Mahmood JJ. evidently considered that the right to privacy could exist in respect of a house in the city of Allahabad. Pro. Winfield in 1931, had to fall back on Indian cases to persuade the House of Commons to extend the right of privacy to British nationals. But the right was not given by recognising right to privacy. This right was given by provisions of trespass and defamation. So the emphasis was only on proprietary rights. It was against the interests of the government to grant right to privacy in full as British were ruling the country. After independence Indian government was following the footsteps of British and right to privacy was not provided under Indian laws. While making the constitution, the constitutional committee also opposed to include this right in the Part III of the constitution as a fundamental right.

3.3 After Independence

Under Indian Constitution, there is no specific enactment for Right to Privacy as such and also there was no legislation for protection of privacy. Therefore the invasion on the right by was challenged on the ground of invasion on right to life and liberty i.e. Art.

21. Various contours of right to life and liberty including right to privacy are explored by the courts. Courts, in many cases touched the various aspects of right to privacy, i.e. against property for search and seizure to disclosure of information and upheld this right under the fundamental right governed under Article 21 i.e. Right to Life and several other provisions of the Constitution read with the Directive Principles of the State Policy. Some of the aspects of Right to Privacy which were given protection by the Supreme Court are discussed in following paragraphs.

3.4 In Context of Search and Seizure

First notable expression of opinion on the 'Right to Privacy' with other

issues of violation of fundamental right under Art. 20 (3) was in decision by Supreme Court in 1954. The power of state for search and seizure was thoroughly discussed and

---

29 Goor Das v. Manohar Das N.W.P.H.C. Rep. 1867, 269 cited in Gokal Prasad (1888) at www.indiakanoon.org/doc/103879 (Last visited on December 11, 2019)

considered by Hon' ble Supreme Court in **M.P. Sharma (1954)**[30], where the allegation was that the company had emblazed the large sum of money and to defraud the shareholders falsified the accounts books. Offences were registered and search warrants were issued to search the documents concerning the property and records were seized. It was alleged that fundamental right of the petitioner under Art. 19(1) (f) and Art. 20(3) are violated because of the searches. The reliance was also put that search and seizure has violated the right to privacy of the petitioner.

The Hon' ble Supreme Court had rejected the contention of violation of fundamental right under Art.19 (1) (f) but considered whether the searches was violating the fundamental right under Art. 20(3). The court observed that the searches were conducted according to the provisions of Criminal Procedure Code. Justice Jaganndhadas observed that searches and seizures do not infringe the fundamental right guaranteed by Art. 20 (3). It was held that if observed carefully, it is evident that search and seizure under Indian law is not termed compulsory. Both are different matters under the law. The notice to produce documents is issued to party concerned and his production is compliance therewith. Person is obliged to submit and therefore production is not testimonial act within the meaning of Art. 20 (3). But search warrant is issued to the police officer, a government servant, who is empowered to conduct the search. So both actions are directed to two different persons. The search and seizure both acts are performed by police officer and the person has to allow the police to conduct search and seizure. So such act of allowance is not testimonial act[31]. It was held that guarantee of self-incrimination is not offended by search and seizure.

The petitioner had relied on the contention that due to search and seizure, his right to privacy is violated and referred the case Boyd v. U.S., in which USA Supreme Court held that incriminating evidence obtained by illegal search and seizure violates the Fourth and Fifth Amendments of American Constitution which provide

for right to privacy. Tracing the history of Indian legislation Supreme Court of India, observed that provisions of search and seizure are contained in Cr. P.C. and conducted after obtaining

---

30 M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077

31 M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077. P. 1096

search warrant. It was held: "In any system of jurisprudence, an overriding power of state for protection of social security and that power is necessarily regulated by law. When the constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of fundamental right to privacy, analogous to the Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of stained construction. Nor is it legitimate to assume that the constitutional protection under Art. 20(3) would be defeated by the statutory provisions for searches" .[32]

The protection was denied in other cases involving the search and seizure under Criminal Procedure Code. The Court denied that it infringes the fundamental right under Art. 20 (3). In

Pooranmal(1974)[33], a search conducted by Income Tax Authorities under s. 132 of Income Tax Act and contention was raised that the search and seizure made by the authorities was illegal.

Dismissing the petition, the Court held that the search and seizure are the powers regulated by Cr. P.C. and in this case the powers were exercised properly and therefore not illegal. It was observed by the Court that the evidence collected by illegal search cannot be excluded on ground that it is invasion of privacy because there is no specific fundamental right to privacy. This decision weakened the right of individual against the illegal search and seizure of the evidence. Moreover Right to Privacy was also de recognised.

This point of view of Supreme Court is also visible in **V.S. Kuttan Pillai (1980)**[11], where again the power of search warrant under s. 91 and 93 of Cr. P. C was under challenge. It was contended that it is violating the fundamental right under Art. 20 (3) of Constitution of India.

32 M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077. P. 1096-97

33 Pooranmal v. Director of Inspection (Investigation) of Income Tax, New Delhi AIR 1974 SC 348 11

V.S. Kuttan Pillai v. Ramkrishnan AIR 1980 SC 185

Supreme Court held that general warrant for searching and seizing listed documents would not entail invasion of privacy even if the search did not yield any result because of counter availing state interests. The Court observed that this is not infringing fundamental right.

The power to gather evidence is extended with the use of advanced techniques. After search and seizure, colling saliva or blood sample was practiced. But with scientific inventions, brain mapping and polygraph tests or lie detector test was conducted by the police. Whether the evidence generated after the reports of such tests invade the fundamental right under Art. 20 (3) i.e. self- incrimination. These tests can result into invasion of privacy of the person as person may lose his freedom or right. The same issue was decided in case of Selvy (2010).

Gathering evidence by using advanced techniques was under scrutiny. In **Selvy (2010)**[34] Supreme Court held that use of narco-analysis, brain mapping and polygraph tests on accused, suspects and witness without their consent is unconstitutional and violation of Right to Privacy. The court referred various decisions given by Hon'ble Supreme Court on Right to Privacy. It had considered the decision given in R (on application of S) v. Chief Constable of South Yorkshire[35], UK, where the Court of Appeal held that retention of fingerprints and DNA samples did not violate the right to privacy provided under Art. 8(1) of the convention as it is justified under Art. 8 (2).

The Judges said, evidence obtained through compulsion is not admitted in evidence. Therefore as these technique produces results which are obtained by compelling the person to go through the test, they violate the right against self-incrimination. Article 20(3) of the constitution protects an individual's choice between speaking and remaining silent, irrespective of whether the subsequent testimony proves to be inculpatory or

34 Selvy v. State of Karnataka, 2010 (7) SCC 263.

35 R. v. Chief Constable South Yorkshire, (2003) 1 All E R (148) (CA) 14

Selvy v. State of Karnataka, 2010 (7) SCC 263.

exculpatory." [14] The bench said, "Article 20(3) aims to prevent the forcible conveyance of personal knowledge that is relevant to the facts in issue.

The result obtained from each of the impugned tests bear a testimonial character and they cannot be categorised as a material evidence." [36] The CJI said, "It is our considered opinion that subjecting a person to the impugned techniques in an involuntary manner violates the prescribed boundaries of privacy and it would be unwarranted intrusion into personal liberty.19" Here the Court held in favour of the person and held that gathering of evidence by employing advance techniques amount to breach of Right to Privacy.

It is important to note that when the R (on application of S) v. Chief Constable of South Yorkshire case was referred to Court of Justice of European Union by the Appellant, (discussed below by the researcher) as UK was part of European Union at that time, the Court of Justice of European Union held that retention of fingerprints and DNA samples after the person is acquitted by the court is breach of right to privacy.

3.5 In Context of Personal Liberty

Right to privacy was judged in the context of personal liberty of the person and decision was given by Supreme Court in following case. Right to Privacy was not well-known till the decision in Kharak Singh was pronounced by the Hon' ble Supreme Court. This was decided for the first time in Kharak Sing' s case and the first tort explained by Prosser i.e. intrusion upon person' s solitude was upheld by Hon' ble Supreme Court.

In **Kharak Singh (1963)[37]**, the Police Regulations in UP were challenged. The petitioner was challenged in dacoity but released as there was no evidence against him. The police opened history sheet against him. Definition of history sheets was provided in Regulation
228 of Chapter XX of U. P. Police Regulations as personal records of criminals under

surveillance. He was put under police surveillance. Under the Regulation 236 of Police Regulation UP, Surveillance involves— a. Secret picketing of house or approaches to the houses of suspects, b. domiciliary visits at night, c. periodical enquiries by officers not

---

36 Selvy v. State of Karnataka, 2010 (7) SCC 263.

37 Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295 17

U.P Police Regulation and Police Act, 1861.

below the rank of sub-inspector into the repute, habits, association, income, expenses or occupation, d. the reporting by constables and chaukidars of movements, absence from the house, e. the verification of movements and absence by means of inquiry sips and also f. collection and record on sheet of all information bearing on conduct[17].

The Petitioner challenged the constitutionality of Chapter XX of UP Police Regulation and in particular Regulation 236. It was also contended by the petitioner that surveillance, and untimely visits of police breached his right to privacy. The case was decided by six judge bench.

In majority judgement, the U.P. Police Regulation was held valid. The petitioner challenged that his right to privacy is violated by late night knock on his door.

When this case was decided, the principles governing the inter-relationship between the rights protected by Art. 19 and the right to life and personal liberty under Art. 21 were governed by the judgement in Gopalan23 case as it considered the right protected under each article as distinct right and not overlapping. The majority judges held because of picketing, the freedom to move freely, guaranteed by Art. 19 (1) (d) was not infringed[38]. It was held that, Art. 21 is not applicable in this situation as right to privacy is not guaranteed in our constitution. So if the police is only ascertaining the movements of the person, it is one of the method, and so is not breach of fundamental right under the constitution[39]. So in Kharak singh also court held that right to move freely under Art.

19 (d) is distinct right and has no relation with right to life under Art. 21.

But domiciliary visits under S. 236 (b) was held invalid as against the right to life protected under Art. 21. Court held that, the word 'personal liberty' shall not be construed to exclude the invasion and intrusion in man's personal security as his right to sleep is a necessity for his existence even as an animal. The court held that in Preamble the words 'dignity of individual' are used and protection of it

ensures the full development of a person. The court held that the words personal liberty shall be construed in a reasonable manner and in the same sense which would promote and

---

38 Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332, para 340

39 Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR (1) 332p. 351

achieve those objectives.[40] It was held by majority that right to life is infringed by the domiciliary visits at night. But the decision was not based on right to privacy.

But in minority judgment given by Subba Rao and Shah JJ that out of other surveillances, surveillance by domiciliary visit was held against the person's right to privacy under Article 21. The Hon'ble Judeges held in minority that by untimely visits, even in night to the house of a person breaches his right to privacy. While discussing the restraints on free movements, the court held that restraints can also be created by certain conditions apart from scientific methods. It was held that personal liberty lies in freedom from encroachment on the personal life of any person and not only from the freedom of movement. The court also reiterates that right to privacy is essential part of personal liberty even though it is not declared specifically by the Constitution.

The court explained that person's own home is very sacred place which provides him rest, physical happiness and security and peace. It is his 'castle'. His home, where he lives with his family, protects his privacy from encroachment by society. The court has stated that what is opined by Frankfurter J., in Wolf v. Colorado [(1949) 238 US 25] about importance of security of one's privacy against arbitrary intrusion by the police, is also applicable to Indian home. The Court held that physical encroachments on his private life would affect it in a larger degree than the physical restraints on his movements. Interference with the privacy is harmful for his health. Therefore it was held that, "We would, therefore, define the right of personal liberty in Art. 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures. If so understood, all the acts of surveillance under Regulation 236 infringe the fundamental right of the petitioner under Art. 21 of the constitutions."[41]

First time it was discussed that whether Right to Privacy could be implied from existing fundamental rights. In a limited way, Hon'ble Supreme Court

recognised that Right to Privacy exists and included in Art. 21-Life and liberty of the person. The ratio

---

40 Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332Pp. 347-348

41 Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332 p.358-359

of Kharak Singh ruled the scenario for more than ten years till in Govind' s case Supreme Court held in favour of the right.

In **Govind (1975)**[42], the Supreme Court assessed more elaborately the right to privacy. The petitioner has challenged the Madhya Pradesh Police Regulation-855 and 856 made under s. 46 (2) (c) of M.P. Police Act, 1961. The constitutional validity of regulation which provides surveillance was challenged. Regulation 855 provides that on information, if the District Superintendent believes that a particular individual is leading a life of crime and the behaviour of that individual show determination to lead a life of crime, that individual' s name may be ordered to be entered in the surveillance register and she would be placed under regular surveillance. Regulation 856 provides that such surveillance may consists of domiciliary visits both by day and night at frequent but irregular interval.

The said Regulation was challenged on two grounds, a. Regulation is not framed under s. 46 (2) (c) of Police Act, 1961 and have force of law, b. even if they are framed under section 46 (2) (c) of Police Act, 1961, provisions regarding domiciliary visits offended Art. 19 (1) (d) and Art. 21.

The court upheld the regulation. It was ruled that regulation is 'procedure established by law', and therefore it is not violating the Art. 21. The Court had observed that Constitution makers were aware of the values propounded by Brandeis J in Olmstead29 relating to spiritual nature, feelings and his intellect. They were also aware about the pain, pleasure and satisfaction from the use of material things. To protect these spheres from the government actions, they have conferred certain space where he should be let alone. [43]

The court accepted the fundamental right to privacy in limited scope emanated from Art. 19(1) (a), (d) and 21. It was also held that this right is not absolute and reasonable

42 Govind v/s State of Madhya Pradesh AIR 1975 SC 1378

43 Govind v/s State of Madhya Pradesh AIR 1975 SC 1378. P.155 24

Gobind v/s State of Madhya Pradesh AIR 1975 SC 1378

restrictions can be placed thereon in public interest under Art. 19(5). The fundamental right can be overridden by the compelling state interest. It was held, "There can be no doubt that privacydignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling state interest test. Then the question would be whether a state interest is of such paramount importance as would justify an infringement of the right." [24]Court had considered the decisions given in cases of Wolf v. Colorado and Griswold along with the European Convention regarding Right to Privacy. Mathew, J, observed that "Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right of privacy is itself a Fundamental Right, the fundamental right must be subject to restriction on the basis of compelling public interest." [25]The court denied the claim of the petitioner.

In changed political scenario, to collect the information about the political rival, tapping of the telephone of him was practiced widely. The same action was practiced by police to gather evidence also. Action of the state by tapping of the means of communication, telephone at that time, was under scrutiny that whether such action implies to invasion of privacy of an individual.

3.6 In Context of Communication Privacy

The Supreme Court's decision in Govind reintroduced the right to privacy into Indian legal system though the regulation was held valid. This protection was extended to another aspects like communication privacy over the period of time. The protection against tort of encroaching the property was extended by recognising the encroachment on communication by one individual to another through telephonic communication. Though the protection was not given under 'Right to Privacy' but the issue of obtaining tapping of telephonic conversion during investigation was considered.

In **R. M. Malkani (1973)[44],** where the police officer, during investigation of case, with the authority of petitioner, attached the tape recorder to his telephone and obtained the evidence of illegal gratification. It was contended by the petitioner inter alia that the evidence of telephonic conversation is obtained illegally in contravention of S. 25 of Indian Telegraph Act and therefore inadmissible as evidence. S. 25 provides that if a person intending to intercept or acquaint himself with contents of any message damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other things whatever, being part of or used in or about any telegraph or in working. It is punished with imprisonment or with fine or with both. The Court observed that the tape recorder was attached to the telephone with authority of the petitioner and therefore there is no breach of the provisions of S. 25 of Indian Telegraph Act and evidence obtained is admissible. The petition was dismissed but Supreme Court stated that telephonic conversation of an innocent person would be protected by the courts against wrongful or high-handed interference by tapping of the telephone conversation by the police. Though it was not linked to right to privacy but the protection was given on the same line as tapping of the telephone is also considered as breach of privacy.

This aspect of privacy, is a personal communication, and by intrusion and invasion on it is by tapping of the telephone was covered under PUCL' s case in detail. Earlier the same issue was discussed in R. M Malkani but as the tapping was done with the permission of the owner, the protection was denied. The question whether tapping of telephone is constitutional was discussed in detail in the case of **People' s Union for Civil Liberties (1997)[45]**. Telephone tapping is permissible in India under S. 5(2) of the Telegraph Act, 1885. The writ petition was filed by voluntary organisation due to mass tapping of the telephones under S. 5(2) of Telegraph Act, 1885 and challenged the constitutional validity of the same.

This section lays down the circumstances and the grounds when an order for tapping of telephone may be passed. The constitutionality of this section has been questioned,

and also no procedure for making the order is laid down therein. On an analysis of s. 5(2),

---

44 R.M.Malkani v/s State of Maharashtra AIR 1973SC 157

45 People' s Union for Civil Liberties v/s Union of India AIR 1997 SC 568, (1997) 1 SCC 301

the Court has concluded that "the first step is the occurrence of any public emergency or the existence of any public safety interest. Thereafter, the competent authority under
s. 5(2) is empowered to pass an order of interception after recording its
satisfaction that it is necessary or expedient to do so in the interest of states etc. same as provided under Art. 19 (2). The authority passing it must be satisfied that the situation is covered under the provision, then the said authority may pass the order for interception of messages,by recording reasons in writing for doing so.

S. 5(2) provides for situations under which the power of interception of messages/conversations can be exercised. But the substantive law as laid down in
S. 5(2) must have procedural backing so that the exercise of power is fair and reasonable. Under
s. 7(2) (b) of the same Act provides that Government may prescribe the rules for taking precautions for prevention of improper interception. But it was highlighted in this case that no such rules were made by Central Government at that time under s. 7 (2) (b) of the Telegraph Act, 1885. (These rules were drafted in the year 1999 after

the Supreme Court decision in the case **PUCL (1997)**[46].

The Court expressed the view that "These rules provide the solid base for the interference of privacy rights for "intrusion upon a person' s solitude or seclusion" and 'information collection' . In absence of just and fair procedure for regulating the exercise of power under S. 5(2) of the Act, it is not possible to safeguard the rights of the citizens guaranteed under Articles 19(1) (a) and 21 of Constitution of India.36 In the course of its judgement, the Supreme Court referred to the International Covenant on Civil
and Political Rights, 1966 to whichIndia is signatory. Article 17 of the Covenant provides for right of privacy and this provision is not conflicting with Article 21 of Indian Constitution. The Court has accordingly interpreted Article 21 inconformity with the International Law.

After considering the judgements of Supreme Court in Kharak sing and

Govind, the Court has ruled in the instant case that "the right to privacy is a part of the right to 'life' and 'personal liberty' enshrined under Article 21 of the constitution. Once the

---

46 PUCL v. Union of India (1997) 1 SCC 301

facts in a given case constitute a right to privacy, protection under Article 21 is extended to them. This right cannot be taken away or lessened except provisions or procedure provided under the law[47]. The Court stated that whether the person can claim such right or not, only depends upon the facts and circumstances of the case. But the person has right to hold a telephone conversation in the privacy of one's home or office without interference. If he does so he can claim as his 'right to privacy'. The Supreme Court has held that conversations on the telephone have an intimate and confidential character being an important facet of personal life of an individual. The court held that such conversations can be protected under Right to privacy. Therefore tapping would infringe Art.21 of the Constitution of India unless it is permitted under the procedure established by law.[48]

The Court has recognised that the conversation on telephone is integral part of person's life and it should not be encroached or invaded without justifiable state interest. In most of the cases above, the state's power to access information by search and seizure or by tapping was challenged. But unauthorised disclosure of information after accessing it by private parties is also breach of right to privacy of an individual. This aspect was also considered in cases discussed below.

3.7 In Context of Personal Information Disclosure

Disclosure of personal information is one aspect where courts guarded the right to privacy. Claims for unauthorised disclosure of personal data or information which breaches the right to privacy are often heard and decided by the Court. Disclosure of information is often done by the media-newspapers or publishers after accessing the personal information to exploit the news. The privacy of person is invaded as reach of the media is vast in comparison to the disclosure through a person.

47 PUCL v. Union of India (1997) 1 SCC 301.p. 311

48 PUCL v. Union of India (1997) 1 SCC 301. P. 311

The invasion by press i.e. publishing the information was raised and discussed in **R. Rajgopal (1994)**[49]. The dispute was regarding the freedom of press and the privacy. The autobiography of a prisoner-a hard core criminal- was to be published by magazine. For this purpose it was alleged that the prisoner has given power of attorney to the publisher. The prison authorities took the objection as names of many high officers were involved in the book. The publisher published three parts in three issues on the magazine. Publisher was under apprehension that police may raid the press and damage the press as it was done on earlier occasion also.

The authorities took objection on the ground that the prisoner had not given any authority to the publisher to publish his autobiography and power attorney is false. Publishers approached Supreme Court for protection of their right under Art. 19 (1) (a), freedom of Speech and expression. The respondents alleged that the names mentioned in the autobiography amount to defamation of the officers. Unauthorised writing of autobiography of one person is breach of right to privacy of that citizen.

The Supreme Court has stressfully pointed out that right to privacy has acquired the status of fundamental right. It is included in Art. 21 as 'right to be let alone'. A citizen has "right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, and education among other matters." [28] The court had tried to reconcile the two fundamental rights, right to privacy and right to speech and expression, which may be in conflict at times. The Court put forward some propositions inter alia:

1. Nobody can publish any personal information, whether critical or praising him or true or not without seeking permission of the person relating to whom the information is published. If anybody publishes it without permission, he is liable for damages as he is violating the right to privacy which is covered under Art. 21.

49 R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632

2. If such personal information is available in public domain or in public records including court records, permission is not required and publication of personal information is exempted as right to privacy is not attached to it."
3. No action for damages in breach of right to privacy can lie against the public officials, if they are discharging their official duties. Otherwise the person has to prove that the publication was false or actuated with malice or personal animosity."
4. State or its officers are not empowered under any law to prohibit or impose restraints on press/media before publication of any information.

The Court had made it clear that the principles above mentioned are only the broad principles. They are neither exhaustive nor all-comprehending. It was rightly pointed out by Mathew, J; that this right has to go through a case-by-case development. We can observe the evolution of the concept 'Right to Privacy' from Kharak Sing[50] to Rajgopal[51], as in earlier case physical privacy was emphasized, and in later case the issue was of reputation of the officers involved and alleged defamation by disclosing information. So the privacy other than physical privacy was targeted.

But where disclosure of information is necessary to protect the fundamental right of another person or the interest of the public then court did not hesitate to hold against the right to privacy. It was evident in **Mr. X (1999)[52]** where the applicant's blood was to be transfused to another but he was tested HIV (+) at the respondent's hospital. On the account of disclosure of this fact, the appellant's proposed marriage to one A, which has been accepted, was called off. Moreover he was severely criticised and was ostracized by the community. The appellant approached the National Consumer Dispute Redressal Commission for damages against the respondents on the ground that the information required under medical ethics, to be kept secret, was disclosed illegally and therefore, the respondents were liable to pay damages to the appellant. The commission

50 Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295

51 R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632

52 Mr. X v. Hospital Z AIR 1999 SC 495, (1998) 8 SCC 296

dismissed the petition on the ground that the appellant should seek his remedy in the civil court.

Before the Supreme Court the appellant contended that the principle of "duty of care" applicable to persons in medical profession included the duty to maintain confidentiality and that the said duty had a correlative right vested in the patient that whatever came to the knowledge of the doctor should not be divulged. The appellant added that for violating that duty as well as for violating the appellant's right to privacy, the respondents were liable for damages to the appellant.

The Supreme Court, while rejecting the appellant's contentions, held that the right to privacy is amassed from Article 21 and other Fundamental Rights read with the Directive Principles of State Policy. The Court observed that this Right may arise outparticular relationship mainly from contract but also including, commercial, matrimonial or even political relationships. Doctor-Patient relationship apart from being commercial, also includes the confidence. Doctors are morally and ethically bound to maintain confidentiality under their professional ethics. In such situation, disclosure of truth about private facts may amount to an invasion of the right of privacy.

This may result into the clash between rights of two persons. Court observed that in this case, one person's 'right to be let alone' with other person's right to be informed is clashed. The right, however, is not absolute and may be lawfully restricted for many purposes including protection of rights and freedom of others. The Court held that in clash of the fundamental rights of two persons under art. 21, the right which promotes the public morality or public interest, will be enforced through court" The claim of the petitioner was rejected.

The information regarding the DNA reports is sensitive personal data. How far this sensitive information be disclosed and whether the person can be compelled to give sample for testing. These question was discussed in **Sharda (2003)**[53].

In the divorce proceedings, the medical examination was ordered for proving the contention of the party.

---

53 Sharada v. Dharampal,(2003) 4 SCC 493

The appellant refused taking umbrage of Right to Privacy under Art. 21. High court decided against the appellant and appellant moved to Supreme Court. It was held that in divorce proceedings, to arrive at proper decision, an order to undergo medical examination on strong ground of necessity to establish a contention. It is necessary to prove or disprove the allegation made. It was held by Supreme Court that if the umbrage of Right to privacy under Art. 21 is taken for avoiding the medical examination which is necessary to evaluate the claims made and defence provided, it is impossible for court to arrive at some definite conclusion on the issue. Moreover it is not absolute right. Court refused to grant relief in favour of the wife.

The important aspect of privacy of individual, i.e. informational privacy was first time traced and tested in true sense by Supreme Court in the case of **Canara Bank**[54] (2005). In this case s. 73 of Indian Stamp Act, 1899 was incorporated by Andhra Pradesh Act,

17 of 1986 by amending the central Act. S.73 of Indian Stamp Act, 1899 empowered the collector or any person authorised by him to inspect the registers, books and records, papers, documents, and proceedings in the custody of any public officer 'to secure any duty or to prove or would lead to the discovery of a fraud or omission. This section was amended by Andhra Pradesh Act, 1986, under which along with the powers conferred under original section, the collector or any other person authorised by him can seize and impound them if it is necessary under proper acknowledgement.

The person who is authorised by collector can seize the documents accessed after giving notice. Statement of Object and Reason to the amended Act provides that as under s.

73 of Indian Stamp Act, 1899, power of seizure and impounding was not provided, the state loses the revenue of stamp duty as documents are not properly stamped or inadequately stamped. Writ petitions were filed by challenging the provisions on

the ground that it is ultra vires to Constitution and inconsistent with Stamp Act and breaching the fundamental right under Art. 14 of the Constitution of India.

High Court of Andhra Pradesh struck down the amended s. 73 of the Act on grounds inter alia that amended s. 73 is inconsistent with other provisions of Act, provision is

---

54 District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496

arbitrary and unreasonable and hence violative of Art. 14 of Constitution. The decision was challenged in Supreme Court on the ground of constitutionality and right to privacy of the persons whose documents are in custody of Banks. After verifying the privacy judgements given by Supreme court of India and United State and privacy right under international conventions, Supreme Court held that, as the ratio in Govind [(1975) 2 SCC 148]is accepted, and in later cases it was held by the court that the right to privacy deals with "persons and not places", the other argument that privacy deals with places and not persons as propounded in Miller[425 US
435 (1976)] cannot be accepted. Even if the documents which are no longer at the customer's house and have been voluntarily sent to bank, they should remain confidential. Unless there is a material which shows to the Collector that documents in possession of bank are lacking in sufficient stamp duty, or there is fraud or omission for payment of the stamp duty, search of the document or taking extract of the document is not valid action. The material must be reasonable for forming an opinion to Collector for issuing an order for search. This safeguard shall be followed while 'action can be taken after forming an opinion' is provided in the law.

3.8 In Context of Freedom of Speech and Expression and IT Act, 2000

The case which has challenged the fundamental right under Art. 19 (1) (a) and not fundamental right under Art. 21 is the case of **Shreya Singhal[55](2015).** Two ladies commented on Facebook, a social media site, about the total closure of Mumbai City after the death of influential political leader. The police arrested both of them under S. 295A of Indian Penal Code and under S. 66A of Information Technology Act, 2000. They were released afterwards and also the cases were dropped which were filed against them. Under S. 66A of Information Technology Act, 2000, law enforcement agencies can arrest and prosecute the person without warrants on the charges. The action raised alarm in the minds of people.

The women filed a petition challenging the constitutional validity of S. 66A of Information Technology Act, 2000 on the ground that it is infringing the fundamental

---

55 Shreya Singhal v. Union of India, AIR 2015 SC 1523

right granted under Art. 19 (1) (a), freedom of speech and expression. The only restriction on the right is provided under Art. 19(2). They argued that provisions under
S. 66A are very vague to restrict the right to comment on the internet which is
covered under right under Art. 19 (1) (a).

Under S. 66 A of IT Act, 2000, if any person who sends message through electronic communication which contain any information which is grossly offensive or of menacing character or the information which he knows it is false but sends it to cause annoyance, inconvenience, danger obstruction, insult, injury, criminal intimidation, enmity etc. or sent for purpose of causing annoyance or inconvenience etc. is guilty. The petitioner contended that the parameters which is restricting the person' s right to expression by sending messages using electronic media are vague. Such parameters shall be in consonance with parameters provided under Ar. 19 (2). The government contended mere chance of abuse of the provision may not be a ground to declare the provision unconstitutional. Legislature is best position to fulfil the needs of the people. Also loose language of the provision cannot be the ground for invalidity because law is concerned with the novel ways to disturb rights of the people through internet. So if the statute otherwise is legislatively competent and non-arbitrary it is valid and cannot be declared unconstitutional.

The Supreme Court held that S. 66 A of IT Act, 2000 is capable of all types of communications on internet. The Court found that it does not make any distinction between mere expression of opinion or discussion and the message which cause annoyance to somebody. The law fails to establish the close relationship with the intention to protect public order. The Court further held that commission of an offence is complete after sending the message. It does not distinguish between the sending it to one person and sending it to masses to create public unrest. The Court held that government failed to show that provisions under S. 66A are for the protection against communication inciting the commission of an offence. The

Court observed that acts pertaining to mere causing annoyance, inconvenience, danger obstruction, insult, injury, criminal intimidation, enmity etc. or merely grossly offensive are not the offences under Indian Penal Code.

For the contention of the petitioner that the provision is vague, the Court verified the United States cases and held that, "the statute which does not lay down reasonable standards for defining guilt in a Section which creates offence and which does not provide any guidance for law abiding citizens or authorities and courts, Section which creates the offence and which is vague shall be struck down". The Court was of the opinion that S. 66A leaves many terms vague and undefined and therefore is not valid. Court observed that by providing for annoyance or inconvenience, it restricts many innocent speeches. The court declared in unconstitutional.

Importance of the case is that that it is deciding the rights of the parties relating to freedom of speech and expression. The court narrowed down the exercise of power under such vague provisions fixing the liability on the persons.

Liability of Intermediary

Avnish Bajaj[56] (2005) is the first case which was decided under provisions of Information Technology Act, 2000, relating to the liability of an Intermediary. This case was decided before the Information Technology Act, 2000 was amended in 2008. In this case, the company Bazee.com was facilitating the business transactions by advertising the goods on its website. The customer who wanted to purchase the goods shall contact the sellers listed on the website. Transactions are completed by both the parties and Bazee.com did not have any role. By advertising on the website, it earns the money. On this website, it was found that pornographic video was put for sale by the name, "DPS Girls having fun".

The filters of website failed to notice it but in manual checking it was observed. After this it was removed from the website but in between this, some purchasers bought videos. The case was registered against the Managing Director of Bazee.com under S.

292 of Indian Penal Code (advertisement or sale of obscene object) and S. 67 of

Information Technology Act, 2000 (causing publication of obscene objects on internet). Delhi High Court came to the conclusion that the Managing Director was prima facie guilty under S.67 of Information Technology Act, 2000 as criminal liability can be

---

56 Avnish Bajaj v. State (N. C. T) of Delhi (2005) 3 Comp.LJ.364 Del. 116(2005) DLT 427

charged against the director under S. 85 of IT Act (offences against companies) where director can be held guilty even company is not charged with. Avnish Bajaj preferred a criminal appeal66 which was heard after tagged with Criminal Appeal 838 of

2008 and it was held by the Supreme Court that the provisions under S. 85 of Information Technology Act, 2000, the director could not be held liable.

Under the provisions of Information Technology Act, 2000, the liability of intermediary is challenged relating to the matter published on website. The case challenging the action under S. 79 of the IT Act, 2000 (before amendment in 2008) is decided exploring the scope in Visaka Industries Ltd. and Ors[57] (2009).

In this case the court verified the liability of intermediary. Visaka Industries are leading manufacturers for asbestos since 1981. They have seven manufacturing plants and twenty five business offices all over India. The defendant Ban Asbestos used to publish the articles on various issues on website hosted by Google Ind. Pvt. Ltd. The contention of the plaintiff was that the defendant has written certain article containing defamatory matter relating to plaintiff Visaka Industries and the said articles were published on the website run by Google which were observed all over the world. Because of these publication, the reputation of Visaka Industries is harmed as such articles are continuously.

The plaintiff by writing to Google India Pvt. Ltd. requested to remove the content from the website. Google India Pvt. Ltd. has answered it is a subsidiary company of Google Incorporation, US and services available on website of Google are not controlled by it. And it is difficult for them to go through each and every article published on their website so they are not responsible for such publication of defamatory matter.

Complaint was filed under S. 79 of IT Act, 2000 and S. 500, 501 of BNS before Metropolitan Magistrate and summons were issued to Google India Pvt. Ltd.

Google India Pvt. Ltd. challenged the decision in High Court. Andhra Pradesh High Court verified the liability of the intermediary which is provided under S. 79 of Information

---

57 Google India Pvt. Ltd. v. Visaka Industries Ltd. Crl. P. No. 7207 of 2009

Technology Act, 2000. It was observed that the responsibility of intermediary is excluded only when such act is committed without the knowledge of him. If he conspires or abet the offence then he will be held liable as he loses his protection under S. 79 (3). Here the High Court found that Google India Pvt. Ltd, did not remove the content even after it was brought to the notice of him. High court found it guilty and dismissed the petition.

After the amendment is carried out in 2008 relating to liability of intermediary, the scope of the responsibility under S. 79 of the IT Act, and IT (Intermediary Guidelines) Rules, 2011 was discussed by the court in **Vyakti Vikas Kendra[58] (2012)**. The case regarding the defamatory statements published regarding His Holiness Sri Sri Ravishankar, owner of The Art of Living Foundation, on blogger.com. This blog was created by the Defendant no.1. The plaintiff no 1. Vyakti Vikas Kendra, India, a Pubic Charitable Trust, is registered Public Charitable Trust which is established to implement and promote the spiritual, educational, social and developmental activities for The Art of Living in India. It filed an action for injunction and damages and also for interim injunction against the defendants.

The court observed that Defendant No. 2 is an intermediary within the definition of S.2 (1) (w) and S. 79 of Information Technology Act, 2000. Under S. 79 (3) (b) of IT Act, 2000, defendant no. 2 is under obligation to remove unlawful content being published through its service. It was also observed that he is also bound to comply with the Information Technology (Intermediaries Guidelines) Rules, 2011. Under Rule 3 (3) along with Rule 3(2), the intermediary is obligated to observe due diligence or publish any information that is grossly harmful, defamatory, libellous, disparaging or otherwise unlawful. Court observed that intermediary shall remove such content within 36 hours of having actual knowledge about such defamatory or libellous content under the rules. Therefore it was ordered by the court to remove all defamatory matter from the website of Defendant no. 2 http:/./blogger.com as well as the

defamatory links within 36 hours.

---

58 In Vyakti Vikas Kendra v. Jitender Bagga, 2012 AIR (Del) 180

So it can be observed that there are few cases relating to intermediary liability and not for right to privacy. The reason may be that people are still not aware about the protection of privacy, which is mostly relating to physical privacy, under the IT Act, 2000. Some rights are included in the right to privacy but they are not included or recognised by IT Act, 2000. One such right is right to be forgotten. Courts provided the protection of this right.

3.9 In Context Of Privacy as a Fundamental Right

Until 2012, it was debated in the various court cases that whether Right to Privacy is fundamental right or not. Supreme Court decided cases on the basis of this right holding that right to privacy is included in Art. 21, but the issue was not substantially and authoritatively decided. The controversy emerged again when government of India has issued uniform identity card scheme for delivery of benefits and subsidies to people. The scheme was opposed as personal information including biometric information was collected for issuing the cards. The Government has established Unique Identification Authority of India under Aadhaar (Targeted delivery of Financial and other Subsidies,Benefits and Services) Act, 2016[59].

J. K.S. Puttaswamy (Retd.) challenged this collection of personal information under Aadhaar scheme. Many cases have filed in the courts all over India challenging this collection by State.

Whether 'Right to Privacy' is to be considered as fundamental right or not, this question arose again when constitutional validity of Aadhaar framework (uniform biometric based identity card) which government wanted to make mandatory for receiving government services and benefits. It was challenged before three judge bench of Supreme Court by retired High Court Judge, **J. K.S Puttaswamy[60] (2012)**. In this petition the collection and use of biometric and demographic information of an individual under Aadhaar scheme was challenged. It was contended that it is violating the fundamental Right to Privacy and therefore invalid. Supreme Court

was asked to decide the validity of

---

59 Act 18 of 2016

60 J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012

Aadhaar Act. The Advocate General of India argued that even though many Supreme Court judgements upheld the right to privacy, but Part III of Constitution does not guarantee this right specifically and separately. Moreover, the larger Supreme Court benches in M. P. Sharma (8 judge bench) and Kharak Singh (6 Judge Bench) also refused to decide in favour of Right to Privacy. As a result of this, the court referred this case to larger bench consisting five judges to ensure "institutional integrity and judicial discipline" .

Again on 18 July, 2017, the constitutional bench presided over by Chief Justice of India was of the opinion that this constitutional question shall be placed before larger bench consisting nine judges to decide the status of Right to Privacy authoritatively. The petitioner argued that Right to Privacy is an independent right included under right to life (with dignity) and personal liberty under Art. 21. The Respondent argued that Constitution provides protection for personal liberties which incorporate Right to Privacy in a limited sense.

The bench consisted Kehar C. J, Agrawal J, Nazeer J, Chandrachud J, Nariman J, Bobde J, Kaul J. Sapre J and Chelameswar J. The judgement of 547 pages contains six opinions and many observations. Justice Chandrachud wrote plurality judgement for four judges (Kehar J, Agrawal J, Nazeer J, and himself). Nariman J, Bobde J, Kaul J, Sapre J and Chelameswar J each wrote separate concurring opinion. The main issue before the court was whether Constitution of India protects Right to Privacy.

The court verified the judgements of M. P. Sharma and Kharak Sing, A.K. Gopalan, R.C. Cooper and Maneka regarding jurisprudential correctness of the decisions after these cases. Various aspects of privacy were addressed to the Court for deciding the matter were: "i) existence of right to privacy under constitution, ii) Whether it is protected as separate fundamental right; iii) the doctrinal foundations of the claim to privacy; iv) the content of privacy; and v) the nature of the regulatory power of the state." [61]

Chandrachud J., while writing the plurality judgement, discussed the concept 'privacy' as discussed by Warren and Brandies. While discussing the concept and its development

---

61 J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P.9

under various legal systems, he referred the doctrines suggested and opinions expressed by the various authors, jurists like Thomson, Posner, Prosser, MacKinnon, Robert Bork, and Alan Westin etc. He also referred the opinions expressed by the Courts in USA from Boyd v U.S (1886) to Florida

v. Jardines (2013) and UK from Prince Albert v. Strange (1849) to R. v. Commissioner of Police of the Metropolis (2011) while deciding the cases relating to Right to Privacy. He compared the concept and provisions regarding privacy under Canada, South African legal system apart from United Kingdom and United States and European Union. He marked some observations about privacy in different systems of society.

He mentioned the development of concept 'privacy' in Indian legal system. For which, he discussed in length the opinions submitted in Constituent Assembly while providing for Right to Privacy in Indian Constitution. He discussed in length the interdependency of the fundamental rights under Art. 14, Art. 19 and Art.21 by taking note of the freedoms under Art. 19 and rights under Art. 21. He did so by reviewing the decisions in A.K. Gopalan, R. C. Cooper and Maneka cases. He held that "the dissenting view expressed by J. Subbarao represents the exposition of correct constitutional position. The jurisprudential foundation in M.P. Sharma and Kharak Singh has been a settled principles in law after these years. He held that these principles include firstly, the fundamental rights emerges from fundamental notions of liberty and dignity. But some aspects of liberty as protected under Article 19 do not deprive the protection under Art. 21. Secondly, state' s action for invasion of any fundamental right under any law shall not be examined on the basis of the object for invasion but it should be examined on the basis of the effects of such invasion on the rights. Thirdly, Constitutional guarantees in Part

III become more meaningful when state action is not arbitrary and is reasonable while exercising the power as per the requirement under Art. 14." [62]

It was held that, "A law within the meaning of Art. 21 must be consistent with

the norms of fairness and equality under Art. 14. As a matter of principle, once

Art. 14 has a connection with Art. 21, norms of fairness and reasonableness would apply to

---

62 J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P. 23, 24.

procedure and law both." [63] It was held that in a same way, right to privacy is not independent of other rights and freedoms guaranteed by Part-III of the Constitution.

How this is applied in judicial review, which is strong remedy, in case of intrusion by state, is the important issue in this judgement. "The guarantee of equality is a guarantee against arbitrary state action. State is restrained from discrimination among persons. The arbitrary action of state violates the equality as such action destructs the body and mind of person. The intersection between one's mental integrity and privacy entitles the individual to freedom of thought, the freedom to believe in what is right, and the freedom of self-determination. Above all the privacy of the individual recognises an inviolable right to determine how freedom shall be exercised." [64] court explained it in the judgment. If the privacy is violated by state action, like exercise of powers of search and seizures, or enacting any law restricting the person then such action or law must be just, fair and reasonable, as it was held in Maneka.

The court had reviewed the decisions given by the Supreme Court on Right to Privacy and discussed various aspects of privacy in those decisions. The Supreme Court has provided protection against the state's power of search and seizure, surveillance, telephone tapping and interception. But the court has discussed the case of Canara Bank[65], in which the court held that the information provided to bank is also protected as privacy is extended to the information provided to the third party. Here the court held that the "privacy attaches to persons and not places." [66]This aspect of privacy, the informational privacy was emphasized by the court in this judgement. Before exploring this the Honb'le court has discussed the concept of privacy.

The concept of 'privacy' is elaborately discussed by the Hon'ble Court in this plurality judgment. The court held, privacy controls the human element which is essential part of human personality. This human element in the personality

enables him to take the

63 J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P. 241

64 J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 243

65 District Registrar and Collector, Hyderabad v. Canara Bank,(2005) 1 SCC 496

66 District Registrar and Collector, Hyderabad v. Canara Bank,(2005) 1 SCC 496, in this judgement at p. 65.

55

J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.242-243

decisions about his personal life which are also crucial to him. By exercising privacy, he keeps alive his thoughts, beliefs, ideas, preferences and choices while dealing with the society. Privacy of the individual is an essential aspect of dignity. Privacy is an element of human dignity and it is inalienable natural right. Dignity is intrinsic value and constitutionally protected interest. Dignity and freedom are inseparable interrelating, each one is a tool to achieve other. By exercising the privacy rights, autonomy of his personality is kept intact by individual. According to the Court it comprises the core of the personality of the individual. It helps to take intimate decisions about himself." [55]

Court observed that "while accessing the internet, personal information or data is exposed. This information or personal data may be accessed or disseminated through data mining. This access or dissemination may result into compromising of interests of the individual. Browsing history of the person can reveal information about not only relating to the person but other persons besides him. It is difficult to think all the possible consequences of uses of internet and its harms." [67]In the judgment it was held that as internet and information technology has opened up new avenues for the communication, information of the person is compromised while communicating through internet. Court focused on informational privacy and while discussing the effects of breach or violation of the personal information or data of the individual, the court took notice of dangers of data mining and Artificial Intelligence on privacy of the person. He stressed that state is under positive obligation to protect the privacy of person and also discussed about the negative and positive obligations of privacy. Negative obligations means state is restricted from interfering unfairly in privacy of person. Positive obligations means State is obligated to enact legislative framework to restrict others from interfering with the privacy of the person.

But according to him, "while maintaining balance between data regulation and individual privacy, the issues of legitimate concerns of state interest

are to be balanced against individual interests in protection of privacy. He explained that proportionality is essential for taking action by the state. Nature and quality of encroachment by state action on the right of the individual shall not be disproportionate

---

67 J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.247-251

to the purpose of law. He held that by protection of informational privacy, human dignity and autonomy to take decisions without interference is protected. He rejected the argument that privacy is an elitist construct." [68]

In this plurality judgement, the Court held that "an invasion of life or personal liberty must meet the three-fold requirement of – i) legality, which postulates existence of law,

ii) need, defines in terms of a legitimate state aim, and iii) proportionality, which ensures a rational nexus between objects and the means adopted to achieve them" [69].

The important features of this judgment is it has recognised that Right to Privacy is fundamental right. Also informational privacy is an important aspect of Right to Privacy in this era of communication technology and internet. State shall take care while acting under the authority of law that such law should be just, fair and reasonable and proportionate for the purpose of the action. State shall protect an individual against the invasion of privacy by enacting laws. This is positive obligation of the state. In the negative obligation, State itself shall not invade the privacy of person.

Five concurring opinions were written by other judges separately. Justice **Chelameswar** expressed the view that the scope of the issue challenged is restrictive. According to him, "three questions should be enquired, i) about existence of fundamental Right to Privacy under constitution of India, ii) if it exists, where it can be found, iii) and contours of such right", while deciding the issue challenged.

While answering the first question, he reviewed the ratio decidendi in the cases M. P. Sharma and Kharak Singh. He also considered the judgements in Boyd and other cases by American court. He expressed his opinion that the minority view in Kharak Singh is the proper one and there is right to privacy under Art. 21. According to him, "the Right to Privacy is an essential ingredient of personal liberty and

decision in M.P. Sharma is not an authority on right to privacy" 83. Court shall interpret the constitution in a manner which would enable the citizen to enjoy the rights guaranteed by Constitution within permissible limits. He pointed out that many rights which were not

---

68 J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.252-253

69 J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.254-255

provided in Constitution are held as fundamental right under Art. 21. So he reiterated the thought that constitution is living document and therefore interpreted accordingly in changing situations.

CHAPTER – 4

LEGISLATIVE FRAMEWORK: RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION IN RESPECT OF USA, CHINA AND INDIA

4.1 Legislative Framework: Privacy And Personal Data Protection In The United States

4.1.1 *Constitutional Foundations and Judicial Development of Privacy in the United States*

The concept of privacy in the United States has evolved primarily through judicial interpretation rather than explicit constitutional recognition. Unlike many modern constitutions, the U.S. Constitution does not expressly guarantee a right to privacy. However, the judiciary has played a transformative role in interpreting various constitutional provisions to derive a broader right to privacy. The First, Fourth, Fifth, and Fourteenth Amendments collectively form the foundation upon which privacy jurisprudence has developed. The Fourth Amendment, in particular, has been central to shaping the contours of informational privacy, as it protects individuals against unreasonable searches and seizures by the state.

One of the earliest and most influential cases in this regard is *Katz v. United States (1967)*,[70] where the Supreme Court held that the Fourth Amendment protects people, not places, thereby introducing the concept of a "reasonable expectation of privacy." This case marked a shift from property-based notions of privacy to a more expansive understanding centered on individual expectations. Similarly, in *Griswold v. Connecticut (1965)*,[71] the Court recognized the existence of "penumbral rights," holding that privacy is implicit in the Constitution. This case laid the groundwork for recognizing privacy in matters of personal autonomy and decision-making.

[70] *Katz v. United* States, 389 U.S. 347 (1967)

[71] *Griswold v. Connecticut*, 381 U.S. 479 (1965).

Further expansion of privacy rights can be seen in *Roe v. Wade (1973)*, where the Court recognized a woman's right to make decisions about her body as part of her privacy rights. Although this decision has undergone significant changes in recent years, its contribution to privacy jurisprudence remains significant. Additionally, *Carpenter v. United States (2018)* addressed modern concerns related to digital privacy by holding that accessing historical cell-site location information constitutes a search under the Fourth Amendment, thereby requiring a warrant. This case demonstrates the judiciary's attempt to adapt traditional privacy principles to contemporary technological realities.

4.1.2 *Sectoral Legislative Framework and Regulatory Approach*

The United States has adopted a sector-specific approach to data protection, which distinguishes it from jurisdictions that rely on comprehensive legislation. Instead of a unified data protection law, privacy in the U.S. is regulated through a patchwork of federal and state laws, each addressing specific sectors or types of data. For instance, the Health Insurance Portability and Accountability Act (HIPAA) governs the protection of medical information, while the Gramm-Leach-Bliley Act (GLBA) regulates financial data. The Children's Online Privacy Protection Act (COPPA) focuses on safeguarding the personal information of children, reflecting a targeted approach to vulnerable groups.[72]

At the state level, laws such as the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), have significantly expanded consumer rights. These laws provide individuals with rights to access, delete, and restrict the sale of their personal data, thereby introducing elements of a rights-based framework within a predominantly sectoral system. However, the absence of a comprehensive federal law has resulted in inconsistencies and regulatory fragmentation, creating challenges for both individuals and organizations.

The Federal Trade Commission (FTC) plays a crucial role in enforcing privacy standards,

primarily through its authority to regulate unfair and deceptive practices. While this approach provides flexibility and encourages innovation, it also limits the scope of

[72] Children's Online Privacy Protection Act, 1998 (COPPA), 15 U.S.C. §§ 6501–6506.

enforcement, as the FTC's powers are constrained by the need to demonstrate harm or deception.

4.1.3 *Case Law Analysis and Emerging Challenges in the United States*

The evolution of privacy law in the United States is deeply intertwined with judicial decisions that address emerging technological challenges. In *United States v. Jones* (2012),[73] the Supreme Court held that the installation of a GPS tracking device on a vehicle constituted a search under the Fourth Amendment, thereby requiring a warrant. This case highlighted the tension between law enforcement practices and individual privacy rights in the digital age.

Another significant case is *Riley v. California* (2014), where the Court ruled that law enforcement officers must obtain a warrant before searching digital information on a mobile phone. The Court recognized that modern smartphones contain vast amounts of personal data, making them fundamentally different from physical objects. This decision underscored the need to adapt legal principles to technological advancements.[74]

Despite these developments, the U.S. framework faces several challenges, including the lack of uniformity, limited protection against corporate data exploitation, and concerns regarding mass surveillance. The revelations by Edward Snowden regarding government surveillance programs further intensified debates on privacy and national security, highlighting the need for stronger safeguards.

4.2 Legislative Framework: Privacy And Personal Data Protection In China

4.2.1 *Evolution of Privacy and Legal Recognition in China*

The development of privacy law in China reflects the country's unique socio-political context, where individual rights are often balanced against state interests. Historically, privacy was not recognized as a fundamental right in China;

however, rapid technological advancements and the growth of the digital economy necessitated the establishment of a

---

[73] *United States v. Jones*, 565 U.S. 400 (2012).

[74] *Riley v. California*, 573 U.S. 373 (2014).

legal framework for data protection. The adoption of the Civil Code in 2021 marked a significant milestone, as it formally recognized the right to privacy and the protection of personal information.

Subsequently, China enacted a series of comprehensive laws, including the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (PIPL) (2021).[75] These laws collectively regulate the collection, processing, storage, and transfer of personal data, while also addressing issues related to national security and data sovereignty. The PIPL, in particular, represents a significant step toward aligning China's data protection regime with global standards, albeit within a state-centric framework.

4.2.2 *Personal Information Protection Law (PIPL) and Regulatory Mechanisms*

The Personal Information Protection Law establishes a comprehensive framework for data protection, incorporating principles such as legality, purpose limitation, data minimization, and accountability. It requires organizations to obtain informed consent from individuals before processing their data and imposes strict obligations on data processors to ensure security and confidentiality. The law also grants individuals rights such as access,correction, and deletion of their personal information.

One of the defining features of the PIPL is its emphasis on data localization and control over cross-border data transfers. Organizations are required to store certain categories of data within China and must undergo security assessments before transferring data abroad. This approach reflects the government's focus on maintaining control over data flows and protecting national security interests. The extraterritorial application of the PIPL further extends its reach, as it applies to entities outside China that process the personal data of Chinese citizens.

4.2.3 *Case Law and Judicial Developments in China*

The implementation of the PIPL has been accompanied by significant judicial developments that clarify its scope and application. One notable case involved a

hotel group that transferred customer data outside China without obtaining separate consent,

---

[75] Personal Information Protection Law of the People's Republic of China, 2021 (PIPL)

resulting in legal action by the affected individual. The court held that such transfers violated the requirements of the PIPL, emphasizing the importance of obtaining explicit and informed consent before sharing personal data internationally . This case underscores the strict approach adopted by Chinese courts in enforcing data protection laws.[76]

Another important development is the decision of the Guangzhou Internet Court, which addressed the extraterritorial application of the PIPL in a cross-border data transfer case. The court held that foreign entities processing the personal data of Chinese citizens are subject to the provisions of the PIPL, thereby reinforcing its global applicability . This decision has significant implications for multinational corporations, as it highlights the need to comply with Chinese data protection laws even when operating outside the country.

Additionally, the case of *Cadence Design Systems Inc. v. Syntronic AB* illustrates the challenges arising from conflicts between Chinese data protection laws and foreign legal systems. The case highlights how restrictions on cross-border data transfers under the PIPL can conflict with obligations under U.S. discovery laws, creating complexities in transnational litigation .[77]

Despite these developments, concerns remain regarding the balance between individual privacy and state control. The Chinese government retains extensive powers to access data for purposes such as national security and public order, which may limit the effectiveness of privacy protections.

4.3 Legislative Framework: Privacy And Personal Data Protection In India

4.3.1 *Constitutional Recognition and Judicial Evolution of Privacy*

The recognition of the right to privacy in India has been a gradual process shaped by judicial interpretation. Initially, the Constitution of India did not explicitly recognize

privacy as a fundamental right. However, the Supreme Court progressively expanded the scope of Article 21, which guarantees the right to life and personal liberty, to include

---

[76] Data Security Law of the People's Republic of China, 2021.

[77] *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.

various aspects of privacy. This evolution culminated in the landmark judgment of Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution .

The Court in this case established a threefold test for determining the validity of any infringement of privacy: legality, necessity, and proportionality. This framework has become the cornerstone of privacy jurisprudence in India, guiding both legislative and executive actions. The judgment also recognized the importance of informational privacy in the digital age, emphasizing the need for robust data protection mechanisms.

Subsequent cases have further expanded the scope of privacy rights. In *Navtej Singh Johar v. Union of India (2018)*, the Supreme Court relied on the Puttaswamy judgment to decriminalize homosexuality, recognizing the right to privacy as integral to personal autonomy. Similarly, in *Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018)*, the Court examined the constitutional validity of the Aadhaar scheme, balancing privacy concerns with the need for welfare delivery.[78]

4.3.2 *Statutory Framework and Digital Personal Data Protection Act*

India's statutory framework for data protection has evolved from the Information Technology Act, 2000, which provided limited protection for personal data, to the enactment of the Digital Personal Data Protection Act, 2023. The IT Act, along with its amendments and rules, introduced provisions related to data security and confidentiality; however, it lacked a comprehensive approach to data protection.

The Digital Personal Data Protection Act, 2023 addresses these shortcomings by establishing a comprehensive framework for the processing of digital personal data. The Act is based on principles such as consent, purpose limitation, data minimization, and accountability. It introduces the concepts of Data Principals and Data Fiduciaries, defining their respective rights and obligations. Individuals are granted

rights such as access to their data, correction and erasure, and grievance redressal.

---

[78] *Justice* K.S. Puttaswamy *(Retd.) v. Union of India*, (2017) 10 SCC 1

The Act also provides for the establishment of a Data Protection Board to oversee compliance and enforce the provisions of the law. At the same time, it allows the government to process data for specified purposes, including national security and public interest, reflecting the need to balance individual rights with state functions.

4.3.3 *Case Law Analysis and Emerging Challenges in India*

The development of privacy law in India is closely linked to judicial decisions that address the challenges posed by technological advancements. In addition to the Puttaswamy case, several other decisions have contributed to the evolution of privacy jurisprudence. In *People's Union for Civil Liberties (PUCL) v. Union of India (1997)*, the Supreme Court recognized the right to privacy in the context of telephone tapping, establishing procedural safeguards to prevent arbitrary surveillance.

In *State of Maharashtra v. Madhukar Narayan Mardikar (1991)*, the Court emphasized the importance of dignity and privacy, holding that even a woman of questionable character is entitled to privacy. These cases demonstrate the judiciary's commitment to protecting individual rights in diverse contexts.[79]

However, the Indian framework faces several challenges, including issues related to implementation, lack of awareness, and the need to balance privacy with national security. The increasing use of digital technologies in governance and commerce has raised concerns regarding surveillance, data breaches, and misuse of personal information. The success of the data protection regime will depend on the effective enforcement of laws, institutional capacity, and public awareness.

Conclusion

The comparative analysis of the legislative frameworks of the United States, China, and India reveals distinct approaches to privacy and data protection, each shaped by unique legal traditions and policy priorities. The United States relies on a fragmented, sector-specific approach that emphasizes flexibility and innovation but lacks

uniformity. China has developed a comprehensive and centralized framework that prioritizes state control

---

[79] *State of Maharashtra v. Madhukar Narayan Mardikar*, (1991) 1 SCC 57

and national security, often at the expense of individual autonomy. India, on the other hand, is attempting to strike a balance between these models by recognizing privacy as a fundamental right while developing a regulatory framework that accommodates economic growth and governance needs.

In the digital age, where data has become a critical resource, the protection of privacy is essential for safeguarding individual rights and maintaining public trust. While each jurisdiction faces its own challenges, the comparative study highlights the importance of developing robust, adaptable, and enforceable legal frameworks that can address the complexities of modern technology. India, in particular, has the opportunity to learn from global experiences and establish a data protection regime that effectively balances individual rights with societal and economic interests.

APTER - 5

CONCLUSION & SUGGESTIONS

The internet, particularly social media, provides a unique avenue for the exchange of distinct ideas, goods and services as well as information. The benefits of these technology cannot be disputed. Technology innovation and excessive, unprotected utilisation of it, however, have the potential to hurt users more severely. In modern digital culture, any information about a person can be transformed into information that can be used to identify him. When privacy is violated or invaded due to the processing of personal data by anyone, including the government, the general public turns to the courts for protection. 80

Hence, in present research work, study was focused on the concept of (personal information) personal data protection with reference to privacy and personal data protection Act , regulations, and rules. This research was done with following objectives-

1. To explore the need to inception of privacy and personal data privacy and the general limitations on right to privacy.
2. To explore the need to inception of Computing advance technology like artificial intelligence in cyber space specially social media. And the instance of privacy breach at social media platforms.
3. To explore the Judicial Response related to Privacy and Personal Data Protection in India .
4. To explore and to find out the legislative framework of privacy and personal data protection in respect of USA, China and India.
5. To find out the technological awareness, and whether social sites are diminishing unity, integrity and social cohesion among users, by collecting

responses from selected field area.

---

[80] General Data Protection Regulation, Regulation (EU) 2016/679.

The study was separated into seven chapters in order to accomplish the aforementioned study objectives. All the objective of study have been addressed. In addition to identifying the objectives and developing the hypothesis, the researcher does a thorough literature study in the first chapter of the introduction.

5.1 Privacy Protection A Serious Concern

Privacy and Personal data Protection in India the definitions and significance of privacy have been carefully examined. To accomplish the study's third objective, this analysis was required which is : to explore the need to inception of privacy and personal data privacy and the general limitations on right to privacy, we can conclude from the above study that there is no precise and universal definition of privacy which can uniformly address all human aspects. Therefore, it has been difficult for many who have tried to define privacy to do so, and some scholars have even given up attempting. "Each person has the legal right to choose how much of himself he wants to disclose with others, as well as when, when, and under what conditions he chooses to do so. It refers to his freedom to take part or leave as he pleases. Additionally, the individual has the constitutionally protected right to regulate the disclosure of personal information about himself which he wants to.

I hold the contrary view, even though many people contend that privacy is an interest rather than a right and that it can impede the common good. Privacy is a unique right, yet it has restrictions in that we cannot mistake one's personal space for another's. This privilege is unalienable to the extent that the individual to whom it has been granted can use it without interference from known or unknown identities. [81]

The modern understanding of privacy has expanded the realm of privacy protection to include many different dimensions. Regarding several aspects of

privacy, there is no legislative classification in place. According to their own viewpoints, several authors categorize it. The protection of anyone's privacy is a critical issue that the

---

[81] Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy", 4 *Harvard Law Review* 193 (1890).

various legal systems must deal with in light of this powerful technological innovation.

This also concluded that "privacy is not an absolute right". It can't go beyond the rights from which it arises. Although the Constitution of India does not have clear or specific provisions for the right to privacy, it is regarded as a right derived from various fundamental rights. Because of this, it is restricted in the same way as other fundamental rights. This right is controlled by certain restrictions as well as other rights. "The limitations can be imposed on this right for the prevention of disorder, crime or protection of morals, health or right and freedom of others".

5.2 Protection Of Personal Data Shared In Social Media Platform Must Needed

Emergence of Artificial Intelligence in social media platforms and instance of privacy breach to address the third and fourth objective of research work e.i to explore the need to inception of Artificial Intelligence based advance technologies in cyber space specially social media and online service platforms, and to explore the incidents of personal data breach.

We get General information of artificial intelligence its application in different fields of life , how it is working in their respective fields and the modern concept of virtual reality adopted by media platforms for better user interface like Meta verse.

An individual can be easily harmed with a computerized data & it can be transferred to third Party. We are not taking it seriously, If our data is publically available than it can be misused. If we fail to secure our Data & Privacy we are at risk of ID theft, phishing scam, voting manipulation can be done by using our data or other risks. We can take example of Cambridge Analytica in America, which used

Facebook likes in order to promote political parties through propaganda. The situation can be worst in a country like India. Our government is storing data related to cast, religion, bank, education etc. all of which can be used for voting manipulation.[82]

[82] Civil Code of the People's Republic of China, 2021

5.3 Conceptual Ambiguity in Privacy Protection

Protection in India, to achieve the fifth objective of the study: to explore the Judicial Response related to Privacy and Personal Data Protection in India, has studied and analyzed several Judgment' s in order to determine the actual status of various laws and regulations on privacy protection in India.

Because there is no specific or distinct law protecting the right to life and liberty, it is protected by Article 21 of the Constitution. The Supreme Court of India has provided and continues to offer protection from violations of the right to privacy in connection to its diverse manifestations. The rights offered by Article 21 are subject to restrictions because its fundamental objective is to shield the individual from the state's arbitrary actions. The court has used all of its creative resources. However, because to the significant growth in commercial information technology use by both the general public and the government, the right to privacy may be threatened in an unprecedented fashion.

In the lack of data protection regulation, there is uncertainty over the protection of personal information and data. The conversation about judicial response makes it clear. The examination of decisions shows that, despite the Indian courts' support for providing redress and justice to regular people who have had their right to privacy and data protection infringed upon or violated, they lack assurance in the absence of clear rules. This was evident when the right to be forgotten was raised before the several High Courts

5.4 Informational Privacy Has a Significant Aspect at the International Level

Legislative framework: Right to Privacy and Personal Data Protection in Respect of U.K, Europe and India, to achieve the fifth objective of the study : to explore and to find out the legislative framework of privacy and personal data protection Law in

respect of U.K, Europe. The researcher studied in detail the laws made in data

protection laws, EU-conventions and General Data Protection Regulation, 2018 and UK-Data Protection Act, 2018. [83]

For the protection of personal data in United Kingdom, the researcher found that United Kingdom has enacted the Data Protection Act, 2018. The impetus is put on protection of personal information (Personal Data). But disclosure of personal information is protected under the breach of confidence as in Douglas. The judgments given by the court show that personal privacy is not provided for. The personal privacy is still protected under tort to property and person or under Human Rights Act, 1992.

For the protection of personal information and data, European Union has provided very strong provisions in General Data Protection Regulation, 2016. And European Union is a step ahead to other countries as they make regulation for artificial intelligence.

For the protection of privacy India has been working since long time when we adopted our constitution. Advancement in information technology is a must-needed requirement for developing.

5.5 Specific Data Protection Legislation: Urgent Need

Privacy Bills in 2011 and 2014 and Personal Data Protection Bills were drafted in 2013, 2018 and 2019, but the absence of statutory law governing privacy and personal data protection is still remain at present time. The detailed analysis of the all the Bills introduced till date has been done. The Privacy Bill, 2019 is the latest on in the series of the various Bills introduced in this context. The Bill was presented in Parliament and presently it is sent to JPC (Joint Parliamentary Committee). Even if it is enacted as an Act these shortcomings which are discussed below are going to affect the right to privacy of an individual.[84]

[83] Data Protection Act, 2018 (UK).

[84] Srikrishna Committee Report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

There are certain lacunain the provisions.

1. While giving protection for data privacy the processing is should to be done in “fair and just” nature. But there are apparent absence of fair and reasonable legal provisions. This is significant because the data fiduciary must be able to demonstrate to the Data Protection Authority that the data had been processed in a fair and reasonable manner. To determine what is "fair and reasonable," the Standard must be offered.
2. In some circumstances, such as when providing services or advantages to the data principal, the state permits the processing of data without consent. This objective is vague. These benefits must be provided without request for processing. It is too broad for the state to grant permission for processing without consent for all public functions.
3. Since private sector businesses performing the same role must get consent, but public sector businesses do not, they do not apply equally to the public and private sectors..
4. Furthermore, "reasonable purposes" also permit processing without consent. These "reasonable intentions" cover a wide range of conditions. These exceptions from the necessity for consent may be subject to abuse by the government. Such power could be applied to surveillance.
5. Any social media intermediary with a user base above a certain threshold may be designated by the central government as a significant data fiduciary if its actions have an appreciable impact on electoral democracy. However, the term "significant impact" is not defined for the purpose of determining whether an impact qualifies as "significant."
6. The concept of "Critical Personal Data," which is not specified in the Bill but is required to be submitted by the Central Government, is another controversial clause. The executives now have extensive power as a result. It looks that the CEOs have been given too much powers in this case as well. As

one of the key definitions for data protection, the researcher contends that what constitutes "Critical Personal Data" must have been included in the Bill.

7. When it is "necessary or expedient" for the reasons listed in the provision, the Central Government is given the authority to exempt any agency of the Government from applying the Act with regard to the processing of personal data. The government might take advantage of or abuse this clause. The phrase "necessary and expedient" enables the state to express a view on the threat that is in its own best interests.
8. It's not quite apparent who has the authority to order the data fiduciary to give government access to non-personal data. It is defined as information that cannot be personally identified. There isn't any additional parameter given. There is a chance that the government itself could put your right to privacy in danger.

Creditworthiness of the parties is a crucial and key component for its successful operation in business transactions or for employment-related objectives. In current information technology era, electronic media and platforms are freely accessible to consumers. It is simple to check the background of someone they intend to do business with or hire. But if the right to be forgotten is granted, it's possible that the person who committed the offences might do them again after they are removed from electronic media, and people connected to him subsequently might suffer as a result. [85]

Additionally, it's possible that this activity will be carried out repeatedly. According to the researcher, this right should not be granted to anyone who has committed a crime of great importance, a terrible crime, or a crime involving moral turpitude. These things are neither considered nor provided for in the Bill.

It is clear from the conversation thus far that there is no legal framework in place to guarantee the privacy of personal data or information generated online. There is a need for a distinct statute that addresses the individual's right to privacy by identifying both government and private party culpability and outlining appropriate remedies. Such a responsible judicial system is a sign of an advanced, democratic

nation.

---

[85] Joint Parliamentary Committee Report on the Personal Data Protection Bill, 2019 (2021).

Although, the privacy bill has been revoked by government after several recommendation get from joint parliamentary committee. And at present no recommendation are available in public domain.[86]

5.6 Gradual Awareness But Still Dependent on Service Provider

The researcher had used non-doctrinal method for fifth objective e.i : tofind out the technological awareness, and whether social sites are diminishing unity, integrity and social cohesion among users, by collecting responses from selected field area, and to meet this end, the researcher used questionnaire as a research tool, which was filled in by stakeholders belonging to Dehradun. The data collected from 512 respondents were analysed and interpreted in **Chapter VI Empirical Analysis ofResponses Collected From Dehradun** of this research work. The inferences are asfollows:

1. The analysis done shows that majority user of internet and social media platform are from age group of 40 to 60 and most of them uses mobile for internet usages.
2. The analysis done shows that time period on social media platform are increasing day by day.
3. Majority of users using internet and social media platform for education and information purposes.
4. Average respondents respondents believes that there photos, signature, mobile number, like and dislike for goods, income, expenditure, religious and political views became data of privacy
5. Majority number of respondent are aware that all social media platforms are gathering their personal data.
6. Majority of users are aware that service provider platforms are gathering user data for economic benefits.

7. Almost every respondent wants to protect their personal data from unauthorized use.

---

[86] Bennett, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United* States (Cornell University Press, 1992).

8. Considerable number of respondent believe that they depend on service provider for their personal data protection. Very less number of respondent believe that they are depend on government for personal data protection.
9. Majority respondents are generally aware of artificial intelligence but not muchn about their future aspects.
10. Almost all respondents are agree on that the advance technology by which user personal data without consent is used can effect society at large.

5.7 Hypothesis Testing

After analyzing the conclusion getting form work research work the both hypothesis which was expected by me are satisfied the hypothesis was

1. **Hypothesis – I** Technological advancement in information technology, like use of artificial intelligence in social medial and online service platforms, made users personal data privacy at stake.

   Conclusion derived from instance of privacy breach and after analyzing responses of the respondents, it is clearly appears that advance technologies in social media and online service platforms made users personal data at stake or solely dependent on service provider in absence of proper legislation.

2. **Hypothesis – II** The Personal Data Protection Bill 2019 needs to enact a robust data protection system by making necessary changes, and privacy protection requires a special governing body which can emphasizes on users personal data protection.

   After through analyzing the conclusion at present time when personal data shared in different platforms is a huge resource for multiple use and government revoke The Personal Data Protection Bill 2019 for necessary amendments after receiving suggestions for joint parliamentary committee. It is high time for government to make a robust and competent legislation regarding data privacy which deal with the platforms on social media

platforms.

5.8 Suggestions

1. India should create a robust data protection law to protect personal data privacy, similar to other developed nations like the European Union, the United States of America, and the United Kingdom.
2. Additionally, the government must be held accountable for breaches in data security and privacy. The government is given various exemptions under the Personal Data Protection Bill of 2019 in relation to its operations.
3. It is necessary to clearly address cloud service providers' liability. The intermediaries and service providers must be held strictly liable. The obligation of cloud service providers must be made clear.
4. The terms imposing liability must not be vague or confusing when defining liability.
5. Provisions governing the government's ability to gather data from intermediaries and service providers must be implemented in a specified manner.
6. Control and rules for the installation and usage of CCTV and biometric data gathering equipment should be specified.
7. A new robust and independent organisation called the Privacy Commission should be established. This panel will examine at the privacy issue and how successfully the law is being applied. It will have investigative powers and will ensure that laws do not become obsolete or modified over time. The Commission should be able to impose its will on the government.
8. "The major reason for the person's limits is the disclosure of data by the individual to the others around him or her." The idea of privacy must include an individual's ability to determine how much information about himself is disseminated. Data disclosure becomes a way of eroding privacy when it is included in the definition of privacy, and so becomes an element of the privacy protection mechanism." The information should be divided into three categories:

"essential data," "sensitive data," and "personal data." "Essential data" refers to information that society has a right to know. Individuals must have the right to keep "sensitive data" private. "Personal data" must include the information.

9. There is an urgent need to pass a comprehensive Privacy Act. The government should form an expert group to investigate incidents of privacy violations and adopt legislation only dealing with such issues. Our government should undertake a public consultation to determine how to improve data protection and privacy safeguards. "The proposed Privacy Act will harmonise, rather than homogenise."The Act should consists enforceable provisions of right to privacy for netizens/citizens, provisions of dynamic grievance redresser mechanism, well defining a deterrence structure in case of noncompliance of rule and regulations, must included a comprehensive effective monitoring mechanism, a suitable and well-explained provision to reduce overlap with other laws
10. Since no clear procedure has been established for such interpretation, other than the Government's ability to intercept under the ISP license, it is unknown how data traffic, especially that which flows over ISP networks, is monitored. Therefore, it is important to have a defined method as soon as feasible for monitoring the data traffic.
11. The law governing data protection must advance along with technology. It should contain exceptions, but they should be strictly outlined and constrained. The law shouldn't be under pressure as a result of the exceptions. "Any restrictions on the right to privacy should be in accordance with the laws now in effect and should only cover those aspects that are required in a democratic state," says the Constitution.
12. Encryption defends against "other attacks," "stealing of data," and "invasion of privacy" for Internet users. “Therefore, the most appropriate and secure method for End-to-end encryption can be achieved by the sender encrypting the communication before it leaves his computer rather than relying on a corporation or firm to accomplish it.. If the data is intercepted, only the hyper text will be visible.
13. To maintain the open internet, international protections and harmonisation must

be implemented. It indicates whether there is a good law. It should be modified and used as inspiration to apply them here. For instance, under the GDPR in Europe, every time you open a website, the website must ask you if they can track you

or not. You have the option to accept or reject. India was the first country to adopt it. Additionally, we will make it clear what information will be tracked and let you decide if you wish to accept it or not.

14. For authorities to gather, use, monitor, and store information, the government should establish explicit procedures. India does not currently have enough privacy protections in place for cases where the government conducts surveillance. Inadequate privacy protection is provided by the current system, which is focused on national security.
15. The use of policies, user agreements, and other terms and conditions must be made clear to end users, and language used should be as simple as feasible. Users should sign agreements that are clear and concise. In order to effectively use data, the user must first be made aware of its origins and intended applications. Consequently, before using or storing data, informed consent is required. Despite declining to share his data, the user still needs authorization to access some websites or resources.
16. A breach of privacy should not just be the responsibility of State actors but also of non-state actors. Legislators need to act right away to safeguard and strengthen the right to privacy as a separate right.
17. Government surveillance ought to be kept to a minimum. The government must realise that privacy is not about keeping information secret; rather, it is about having the freedom from unauthorised interference.
18. The management of other government programmes and the distribution of subsidies should be handled by programmes like Aadhaar, but they shouldn't turn the system into a surveillance State. To reduce identity theft and prevent other types of forgeries, Aadhaar's security and privacy protections should be strengthened.
19. Strict penalties for privacy violations should be included in the law, but for the time being, it is important to ensure that the law does not unnecessarily hamper practical technological advancements.

There is a apperent urgent need to understand that data which is collected is not evaporating rather it is collected. By sharing personal information of people and users with interested firms turned into trillion dollars of profits by service provider firms

last years and this business is increasing day by day. And advance tool like machine learning in data profiling accuratly and prudently predict personality, drives behaviour, and influence how to caste you vote, buy, eat, etc. only to gain more monitory benefits. So, the government need to regulate these unethical practices not only nationally but internationally also in every platforms.

In border sense every individuals should be made their self aware of privacy problems while using any social media platform, mobile app, commercial site as over half of the country's population has access to the internet. We had nearly 700 million internet users in last year' s, and that number is expected to increase to million or may be more by 2025. It is imperative that individuals become informed and well aware with data breaches and how they affect their rights.[87]

Meanwhile, privacy jurisprudence remains a source of worry across the world. Individual independence and liberty have been pushed for by the rise of liberal democracy and the internationalization of human rights. And technical advancements in IT(specially artificial intelligence), particularly in the fields of media, communication platforms in cyber space, have had an major influence on privacy issues. Debates regarding the nature of privacy will intensify, making the subject an interesting issue to research. Privacy is conceivable in the digital era which is developing into virtual reality ; all we need is the confidence that it is possible. It is a work in progress, and there is still more to be done.

[87] Schwartz, Paul M. and Solove, Daniel J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 *New York University Law Review* 1814.

References:

1. Ratanlal & Dhirajlal, *The Indian Penal Code* (29th edn., Wadhwa & Co., Nagpur, 2003).
2. K.I. Vibhute, *P.S.A. Pillai's Criminal Law* (11th edn., LexisNexis Butterworths, Nagpur, 2012).
3. K.D. Gaur, *Criminal Law: Cases and Materials* (6th edn., LexisNexis, New Delhi, 2016).
4. Bimal Raut, *Judicial Jurisdiction in Transnational Cyberspace* (New Era Law Publications, Delhi, 2004).
5. Rodney D. Ryder, *Guide to Cyber Law* (2nd edn., Wadhwa & Co., Nagpur, 2003).
6. Barkha U. Ram Mohan, *Cyber Law and Crimes* (3rd edn., Asia Law House, Hyderabad, 2011).
7. K. Sita Manikyam, *Cyber Crime: Law and Policy Perspectives* (Hind Law House, Hyderabad, 2009).
8. S.C. Sarkar, *The Code of Criminal Procedure* (8th edn., LexisNexis, New Delhi, 2004).
9. Vimlendu Tayal, *Cyber Law, Cyber Crime, Internet and E-Commerce* (Bharat Law Publications, Jaipur, 2011).
10. Information Technology Act, 2000 (India).
11. Information Technology (Amendment) Act, 2008 (India).
12. Indian Penal Code, 1860.
13. Code of Criminal Procedure, 1973.
14. Indian Evidence Act, 1872.
15. *State of Maharashtra v. Mohd. Yakub*, (1980) 3 SCC 57.
16. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
17. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
18. UNCITRAL Model Law on Electronic Commerce, 1996.
19. Council of Europe, *Convention on Cybercrime (Budapest Convention)*, 2001.
20. Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce*

(Universal Law Publishing, New Delhi, 2002).

21. Talat Fatima, *Cyber Crimes* (Eastern Book Company, Lucknow, 2001).
22. Aparna Viswanathan, *Cyber Law: Indian and Internatio Perspectives* (LexisNexis, 2007).
23. Vivek Sood, *Cyber Law Simplified* (Tata McGraw-Hill, New Delhi, 2001).
24. Nilakshi Jain, "Cyber Crime and Legal Framework in India" (2013) 2 *International Journal of Law and Legal Jurisprudence Studies* 1.
25. Pavan Duggal, "Cyber Law in India: An Overview" (2002) 1 *Indian Journal of Law and Technology* 1.
26. *Katz v. United States*, 389 U.S. 347 (1967).
27. *Griswold v. Connecticut*, 381 U.S. 479 (1965).
28. *Roe v. Wade*, 410 U.S. 113 (1973).
29. *Carpenter v. United States*, 585 U.S. (2018).
30. *United States v. Jones*, 565 U.S. 400 (2012).
31. *Riley v. California*, 573 U.S. 373 (2014).
32. Health Insurance Portability and Accountability Act, 1996 (HIPAA), Pub. L. No. 104– 191.

33. Gramm-Leach-Bliley Act, 1999, Pub. L. No. 106–102.
34. Children's Online Privacy Protection Act, 1998 (COPPA), 15 U.S.C. §§ 6501–6506.
35. California Consumer Privacy Act, 2018 (CCPA), Cal. Civ. Code § 1798.100.
36. California Privacy Rights Act, 2020 (CPRA).
37. Cybersecurity Law of the People's Republic of China, 2017.
38. Data Security Law of the People's Republic of China, 2021.
39. Personal Information Protection Law of the People's Republic of China, 2021 (PIPL).
40. Civil Code of the People's Republic of China, 2021.
41. *Cadence Design Systems Inc. v. Syntronic AB*, No. 20-cv-03689 (N.D. Cal. 2021).
42. Information Technology Act, 2000 (India).
43. Information Technology (Reasonable Security Practices and Procedures and

Sensitive Personal Data or Information) Rules, 2011.

44. Digital Personal Data Protection Act, 2023 (India).
45. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
46. *Justice K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1.
47. *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.
48. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
49. *State of Maharashtra v. Madhukar Narayan Mardikar*, (1991) 1 SCC 57.
50. General Data Protection Regulation, Regulation (EU) 2016/679.
51. Data Protection Act, 2018 (UK).
52. Human Rights Act, 1998 (UK).
53. Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy", 4 *Harvard Law Review* 193 (1890).
54. Solove, Daniel J., *Understanding Privacy* (Harvard

University Press, 2008).

55. Greenleaf, Graham, *Asian Data Privacy Laws: Trade and Perspectives* (Oxford University Press, 2014).
56. De Hert, Paul and Papakonstantinou, Vagelis, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" (2016) 32 *Computer Law & Security Review* 179.
57. Srikrishna Committee Report, *A Free and Fair Digital Eco Privacy, Empowering Indians* (2018).
58. Joint Parliamentary Committee Report on the Personal Data Protection Bill, 2019 (2021).
59. Bennett, Colin J., *Regulating Privacy: Data Protection and Europe and the United States* (Cornell University Press, 1992).
60. Schwartz, Paul M. and Solove, Daniel J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2

011) 86 *New*

University Law Review 1814.