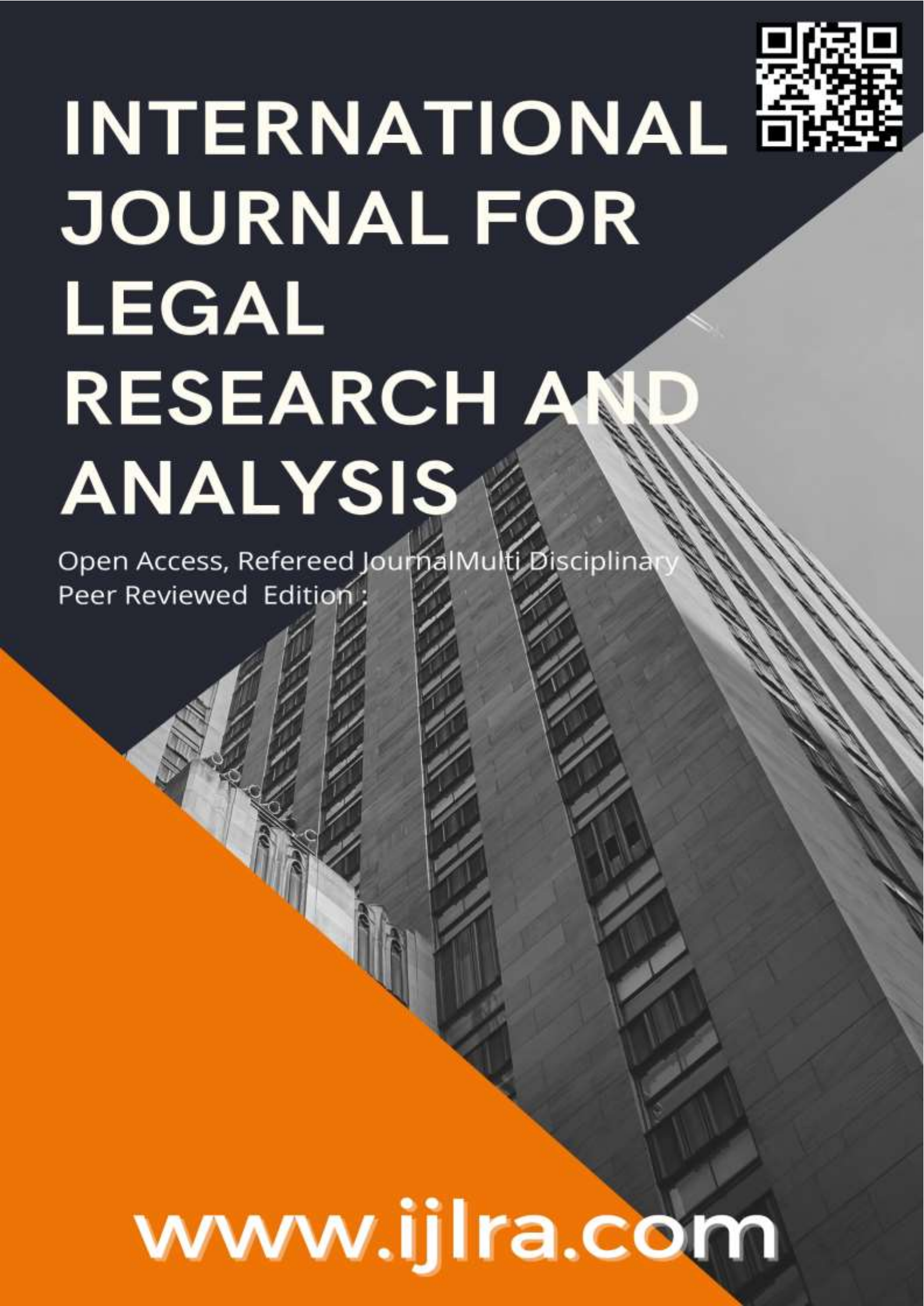
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :



www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

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

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

Dr. Samrat Datta

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

 ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

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

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

Mrs.S.Kalpana

Assistant professor of Law

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

Avinash Kumar

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

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

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

 ISSN: 2582-6433

RIGHT TO PRIVACY AND DATA PROTECTION ISSUES: A CRITICAL STUDY WITH REFERENCE TO KS PUTTASWAMY VS UNION OF INDIA JUDGEMENT.

AUTHORED BY: BABAR KHAN & DR. TARU MISHRA
AMITY LAW SCHOOL,
AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

ANTI-PLAGIARISM CERTIFICATE

It is certified that the dissertation titled as "**RIGHT TO PRIVACY AND DATA PROTECTION ISSUES:A CRITICAL STUDY WITH REFERENCE TO KS PUTTASWAMY VS UNION OF INDIA JUDGEMENT**" by **BABAR KHAN** has been examined with the following anti-plagiarism tools.

We undertake the following:

I. That the dissertation has been checked using Amity University subscribed ***Turnitin***, an anti- plagiarism software to check the documents of students and scholars for detecting plagiarism, and found within limits as per University Norms .That the dissertation has significant work/knowledge as compared already published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced;

II. That the work presented is original and own work of the author i.e. there is no plagiarism. No ideas, processes, results or words of others have been presented as author's own work.

III. That there is no fabrication of data or results which have been complied and analyzed; and

IV. That there is no falsification by manipulating research materials, equipments or process, or changing or omitting data or results such that the research is not accurately represented in the research record.

 ISSN: 2582-6433

BABAR KHAN
RESEARCH SCHOLAR

DR.TARU MISHRA
RESEARCH SUPERVISOR

CERTIFICATE

I hereby certify that-

(a) Babar Khan, A8101823082 Sudent of LL.M (2023-24) at Amity Law School, Amity University Uttar Pradesh has completed the Project Report on "**RIGHT TO PRIVACY AND DATA PROTECTION ISSUES:A CRITICAL STUDY WITH REFERENCE TO KS PUTTASWAMY VS UNION OF INDIA JUDGEMENT"** during **2ND semester** under my supervision.

(b) The presented work embodies original research work carried out by the student as per the guidelines given in University Regulations.

(c) The Research and writing embodies in the thesis are those of the candidate except where due reference is made in the text.

(d) I am satisfied that the above candidate's prima facie, is worthy of examination both in term of its content and its technical presentations relative to the standards recognized by the university as appropriate for examination.

(e) I certify that in accordance with NTCC guidelines, the report dose not exceed the prescribed maximum word limit; or prior approval has been has been sought to go beyond the word limit.

(f) Wherever work from other source has been used, all debts(for words, data, arguments and ideas) have been appropriately acknowledge and referenced in accordance with the requirements of the NTCC Regulations and Guidelines.

SIGNATURE OF THE FACULTY
DR. TARU MISHRA
ASSISTANT PROFESSOR
AMITY LAW SCHOOL

 ISSN: 2582-6433

DECLARATION

Title of Project Report "**RIGHT TO PRIVACY AND DATA PROTECTION ISSUES:A CRITICAL STUDY WITH REFERENCE TO KS PUTTASWAMY VS UNION OF INDIA JUDGEMENT**".

I understand what plagiarism is and am aware of the University's policy in this regard.

…….

I declare that

(a) The work submitted by me in partial fulfillment of the requirement for the award of degree LL.M. Assessment in this Dissertation is my own; it has not previously been presented for another assessment.

(b) I declare that this dissertation is my original work. Wherever work from other source has been used, all debts(for words, data, arguments and ideas) have been appropriately acknowledged and referenced in accordance with the requirements of NTCC Regulations and Guidelines.

(c) I have not used work previously produced by another student or any other person to submit it as my own.

(d) I have not permitted, and will not permit anybody to copy my work with the purpose of passing it off as his or her own work.

(e) The work conforms to the guidelines for layout, content and style as set out in Regulations and Guidelines

Date: 24/04/2024 **Babar Khan**
A8101823082
LL.M

ACKNOWLEDGEMENT

The ability to complete my dissertation had its origins before the commencement of my formal studies at Amity Law School, Amity University. Without the benefit of so many great interactions with people throughout my life, this path might not have opened up for me to pursue. As such, it is necessary to reach back and thank a great number of people. To acknowledge everyone, is a formidable undertaking and I make no apology for the length of these acknowledgement. It is loosely presented in chronological order, with overlap in names reflective of multiple influences

 ISSN: 2582-6433

certain people have had on my journey. First of all I thank to my God who gave me that much capacity and made me able by giving adequate intellect so that I got succeed in making my dissertation. Now I would like to thank my mentor and guide **DR.TARU MISHRA** , faculty of law, for selecting me to work on this research and guiding me throughout. I thank her for his intellectual guidance throughout my dissertation more as an academician. Thanks to my mother, Mrs. **Afgana Khan**, for teaching me to love learning and letting me know that how to present myself in the various chapters of life. Thanks to my father **Mr. Sahare Khan**, for teaching me activeness, presence and confidence. I would undoubtedly like to thank my friends who helped me in the completion of the work and all my well wishers who had helped in the completion of this work.

BABAR KHAN
A8101823082

PREFACE

Chapter One: Introduction: In this chapter, the researcher includes the introduction, research methodology, literature review, hypothesis, significance of the Right to Privacy and Data protection in India. He has also studied the objectives behind the research conducted on the Privacy Right and Data Protection in India. This chapter includes the general overview to the concept of privacy right as an essential right of the citizens and also the problem faced by this right in today's era of information and data.

Chapter Two: Right To Privacy and Data Protection in General: In the second chapter the researcher has included the general overview of the Right to Privacy and Data Protection. The chapter includes the elaborative explanation of the concept of privacy and some dictionary and scholarly definitions of privacy right. The chapter includes the root or the origin of the privacy right and its development in different times. Privacy and its presence in different dimensions are also included in this chapter.

 ISSN: 2582-6433

Chapter Three: Legal Framework Relating to Privacy and Aadhaar Act, 2016: In the third chapter the researcher talks about the law's presently operating in India in regard to the privacy and the data protection. The chapter includes all the constitutional provisions which are considered to be connected to the privacy specifically Article 19 and Article 21. All the different legislations like Information Technology Act, Hindu Marriage Act, Indian Penal Code, Indian Easement Act, Copyright Act, Children Act, Credit Information Companies (regulations) Act, Right to Information Act, Evidence Act and many more are also included in this chapter. The researcher also included in this chapter several schemes like 'Unique Identification Scheme' and 'NPR Scheme'. Moreover the chapter also includes the expert committee's recommendations and the Draft Bills relating to Data Protection.

Chapter Four: Judicial Approach with special focus on Ks Puttaswamy vs UOI Judgement: In the four chapter, the researcher focuses on the approach regarding the right to privacy and protection of data, followed by the judiciary. This chapter deals with the various case laws especially **Puttaswamy** judgement which reflect the attitude of the Indian judicial system about the privacy rights in the Indian society. It also analyzes the recent development towards the privacy as a fundamental right. And it also talks about present threat in the protection of data in this cyber society. This chapter shows the efforts taken by apex court to prohibit the breach of the right to privacy to maintain the essence of the constitution in the country.

Chapter five: Conclusion & Suggestions: In the Last chapter, the researcher finally concluding the topic by giving various suggestions to the concept of Right to Privacy and Data protection in the country and also throw light on the present scenario followed by the society and its impact on the modern society. It also describe the following recommendation so that to improve the condition in the India and also to adopt the firm and efficient legal framework so that to achieve the goal to provide protection of data from any kind of mishappening.

 ISSN: 2582-6433

LIST OF ABBREVIATIONS

AIR	All India Reporter
Art.	Article
CBI	Central Bureau of Investigation
CD	Compact Disc
CEDAW	Convention on the Elimination of all Forms of Discrimination Against Women
Cr.P.C	Criminal Procedure Code
CLJ	Criminal Law Journal
Ed.	Edition
EEOC	Equal Employment Oppurtunity Commission
etc.	Etceteras (and so forth)
FIR	First Information Report
FWFPR	Female Work Force Participation Rate
Har.L.Rev	Harvard Law Review
HC	High Court
HRD	Human Resource Development
LAWS	Indian Association for Women's Studies
Ibid	Ibidem (in the same place)
ICCPR	International Covenant on Civil and Political Rights
ID Act	Industrial Disputes Act
ILO	International Labour Organisation
IPC	Indian Penal Code
IT Act	Information Technology Act
MMS	Multimedia Messaging Service
MSPB	Merit System Protection Board
NCERT	National Council of Educational Research Training
NCRB	National Crime Report Bereau
NCW	National Commission for Women

 ISSN: 2582-6433

NGOs	Non- Governmental Organisations
NHRC	National Human Rights Commission
PUCL	People's Union for Civil Liberties
RAF	Rapid Action Force
SC	Supreme Court
SCC	Supreme Court Cases
SCD	Supreme Court Digest
SCJ	Supreme Court Journal
SCW	Supreme Court Weekly
SDA	Sex Discrimination Act
Sec.	Section
SHW	Sexual Harassment in the Workplace
UK	United Kingdom
UNESCO	United Nation Educational Scientific & Cultural Organisation
UNGA	United Nations General Assembly
UNO	United Nation Organisation
USA	United States of America
Vol.	Volume
WPR	Work Participation Rate

 ISSN: 2582-6433

TABLE OF CASES

 ISSN: 2582-6433

 ISSN: 2582-6433

CONTENTS

 ISSN: 2582-6433

 ISSN: 2582-6433

 ISSN: 2582-6433

CHAPTER: ONE

 ISSN: 2582-6433

INTRODUCTION

1.1 GENERAL OVERVIEW

When a society has distinguished between the "external" and the "internal"; between the existence of the conscience and the existence of the bodies; among the mystical and the abstract; the godly and the god-less; the world of Lord and the world of Man; the Place of worship and the Government; between certain fundamental and sacrosanct privileges and the right of state to provide and deprive; between private and public; among community and isolation; it becomes unavoidable the presumption of personal freedom by any name it could be called-the concept of "personal space where a person can be what he/she wants and stay that way."[1]

Privacy is a person's most vital need to set-out the personal limits and prohibit another's introduction to the same area. In both Asian and Western cultures, there is adequate proof to promote this perspective. The concept of privacy is as ancient as the times of the Bible. Animal conduct and social institution research indicate that any kind of need for privacy of a person may well be grounded in the heritage of creatures, and therefore that people and creatures share a few fundamental principles for demanding privacy among their companions.[2] The Holy Bible states the time when Adam and Eve opened their eyes and they knew that they were naked, so they stitched together the leaves from the trees and made clothes for themselves.[3] It might have taken thousands of years to navigate the gap from the mythological garden to the statutory wilds, because it is necessary to determine a safe relation among people whether it is between married couple, father and son or among friends. In certain terms, it concertizes affection, trust, and friendship relations. In its general sense, the idea of privacy includes a range of dimensions, such as non-disclosure of personal data, personal affairs, privacy of secrets related to business and non-inclusion of someone else, etc. It is a notion of isolation, confidentiality and independence. Privacy is an indissoluble component of every culture's heritage.

"Privacy" has turned out to be a broader idea. Considerably autonomous have enslaved the conventional freedoms, secrecy, defamation, assets and the retention of information.[4] The privacy rights could therefore involve disclosure of personal events publicly and the interference into the

[1] Herbert Marcuse, *Privacy And The Law : A Philosophical Prelude* 273 (Oxford University Press, London, 1966)
[2] Alan F. Westin, *Privacy and Freedom* 8 (Princeton University Press, New York, 1970)
[3] S. K. Sharma, *Privacy Law : A Comparative Study*, 25 (Eastern Book Publishing, New Delhi, 1994)
[4] *Supra note 3 at p. 1*

 ISSN: 2582-6433

isolation, or personal affairs of people.[5] The modern government gathers all kinds of personal data and often store this data in a computerized manner. Two kinds of problems can be foreseen in that kind of scenario. One concerns the person's fear of publishing it by the authorities. The other concerns the agency's risk of supplying such information to outsiders. In both instances, prior to any possible publishing, the person's approval is not received. After the publishing, the person involved comes to notice about everything. Even though the agency's privacy rights save's the individual from any publishing, it prevents the strangers from providing such data.

There is a core faith in the person's individuality, his inherent integrity, his value as a living being in the democratic communities. The growth and retention of the feeling of individual identity has been correlated by psychologists and social scientists to the individual need for freedom. Another of the recognized methods of depicting a need for an absolute component of independence for the person was to establish relation between the person and those around him in context of a series of privacy or areas leading to a 'Self identity.' This "self identity" is portrayed as a sequence of successive layers surrounding it. The internal circle protects the essential truths of the person, those aspirations, concerns and ambitions which are beyond exchanging with someone unless the person is so pressured that he will have to put out such essential truths to ensure emotional faith. Most severe danger to personal freedom is that, somebody will enter his private space and will either by material or some other methods discover these essential secrets. This purposeful breach of the security shell of a person, his emotional shield will leaves him exposed to insults and puts him behind the command of all those who know his secret information.

The concept of privacy as a 'right' emerged in the United States of America when the American researcher Cooley described this as a highly vague notion as, merely by identifying it as the 'privilege to be left alone.'[6] A few years after, Samuel and Louis developed the idea with the original analysis of the concept of privacy.[7] The type of concern, which privacy aims to safeguard, is still confusing. There seems to be a discipline of philosophy whose most exceptional representative is Dean Prosser. According to him privacy was not an autonomous element at all, but a blend of interest in prestige and emotional peacefulness with intangible assets. Dean Prosser's perspective was accepted by Salmond in his work "Law of Torts,"[8] although in instances

[5] Raymond Wacks, *Personal Information Privacy and the Law* 20-21 (Oxford University Press, London, 1994)
[6] Thomas M. Cooley, *Law of Torts* 91 (Oxford University Press, London, 1888)
[7] Samuel D. Warren, "The Right to Privacy", 4 HLR 193 (1890)
[8] John William Salmond, *The Law of Torts*, 44-46 (Arkosh Press, London, 15th edn., 2015)

 ISSN: 2582-6433

where American judiciary do recognize the English common law would not acknowledge privacy intrusion as a torture. The three separate torts that are found in these instances, according to Dean Prosser, are:

- Encroachment into, the solitude or isolation of an individual.
- Public exposure of a individual's personal life's unpleasant details.
- Grant to the benefit of the title or image of another individual.

Protected interests in these instances are interests in liberty from emotional distress, public exposure and misleading cases, interest in prestige and in appropriation cases, ownership interest in the title and resemblance. From this perspective, the precious 'right to privacy' constricts in its importance and it will become a mere implementation of conventional legal freedoms to novel conditions to preserve well-identified and well-established societal values.[9] Privacy isn't really, in the above perspective, an autonomous legal right that protects an essential human quality. Privacy assaults are transformed into a kind of abuse, emotional distress, and misuse. Accordingly, there is no new practice of violation of privacy, yet only unique methods to undertake outdated torts. In several other terms, the personal value or concern in security is not an autonomous one, but only a mixture of the significant community position on protecting the emotional, peacefulness, prestige or intangible types of property.

Developing the definition of privacy has made quick progress with latest science and technological advancements and has lifted the possibility of unique and terrifying privacy attack on one's house without his permission or even understanding. Due to these innovations, a man's home with the help of advanced machines is no longer untouched or safe from phone-tapping and spying.[10]

A privacy right preserves one's personality, dignity and intimacy with regard to the region of a personal life. Identification involves the name, race, image, feelings, honour, prestige, etc. Moreover, privacy isn't an utter right. Even unfair or illegitimate intrusion is discouraged; in order to better understand if a specified intrusion encroaches upon the privacy right, it must be balanced with other essential concerns, such as nation's security, health, morality, crime's prevention or the rights and liberties of the others. This same applies if transsexuals are prohibited from modifying gender by nations. However, forced medical procedure that disrupts with the dignity of the person

[9] *Ibid*
[10] Justice R. S. Sarkaria, "Freedom of the Press: Defamation and Privacy", 15 PCIR 96 (1994)

 ISSN: 2582-6433

may be encouraged in the concern of other people's freedoms, as in the event of compulsory blood withdrawal for the reason of deciding parental rights. Intimacy is also at the root of privacy and implies that several personal traits, actions or information should be held confidential. Provided that, the accusations that electronic information processing poses to privacy, countries are obliged to accept data protection legislations with effective administrative methods. Intrusion with intimate life and independence could not be tolerated on ethical or safety grounds alone. Consequently, both the European Court of Human Rights and the Committee on Human Rights discovered a particular ban on homosexuality to be a breach of the right to privacy[11].

The Universal Declaration of Human Rights, the Covenant on Civil and Political Rights, the European Convention on Human Rights and the other regional Conventions on Human Rights in preparing of different regions of the world outside Europe ensure appreciation for a individual's personal and family life, his house and communications in almost equivalent concepts. This concept might seem to be self-evident, as this is one of those we discover at the beginning of the concept of human rights, and is one of the pillars of democracy as it originated from Magna Carta and other human rights declarations. The person in a social order needs to strike a harmony among freedom and discipline. There has been an issue in system of surveillance, and when a large organization can utilize them for political or industrial intelligence the outcome can be spectacular. On the other hand if the techniques are used by police or private investigators or press on the individual they can surely humiliate and discomfort the person. Also, in spite of the fact that although to some degree can be countered, some of them are at times necessary, broad use would make life meaner. All people would have constantly to live in a condition of strain, even those who have nothing to hide up. The dislike of surveillance is instinctual; even well expected parental surveillance ends up irritating. Maybe everything returns to some primitive ancestor who realized that the main eyes which tailed him continuously were those of a stalking predator.[12]

In the meantime, the risks of surveillance is ought not to be seen out of perspective. The facts confirm that any given individual could be exposed to embarrassingly penetrating surveillance, however the expense is high to the point that just a little extent of people could be kept under the surveillance constantly, even in an extremist state. In spite of the fact that, the new surveillance gadgets would be a guide to a dictator or to the ruling party, it is important for a free

[11] Javed Dhar, *Privacy & Data Protection Laws in India*, 44 (Independently Published, New Delhi, 2018)
[12] G.B.F. Niblett, *Privacy and Human Rights* 73 (Oxford University Press, London, 1972)

 ISSN: 2582-6433

society to realize that these aids to dictatorship and to exist with the goal that it can be on its guard, and what is essential to that society is that it must have enough men of foresight and strength to oppose tyranny, regardless of whether actually helped or not.[13] The same applies to every other type of danger to privacy i.e. the cross examination under pressure, identity tests, data banks and tempering with the inner mind. The expansion in the flow of data induced by the computer threatens the person's capacity to control the flow of information about himself at the end of the day, his privacy is endangered. Without a doubt new laws are required. During 1968 a private member's bill i.e. the Data Surveillance Bill, was presented in the House of Commons with the point of giving legislation 'to prevent the intrusion of privacy through the abuse of computer information.' The bill did not progress toward becoming law but rather all things considered included fascinating new recommendations, for example, registration of computer operated information banks and the necessary supply of printouts which might be embodied in future enactment. A few federal statutes confine the gathering, stockpiling, and appropriation of data, for instance, the Privacy Act of 1975 directs the accumulation and utilization of personal data controlled by the national government. The Act allows the legislature to gather only the "important" or "necessary" data and limits of revelation of person's records.[14]

However, the Act explicitly restricts its provisions from disallowing the release of any material for which exposure is required under the Freedom of Information Act. "The Freedom of Information Act" enables private citizens to get access to government records, subject to a few exemptions. Also, the 'Privacy Act' just controls data assembled by the administration and does not have any significant bearing to individual data gathered and disseminated by private entities. In America, the Congress managed the issue of States selling driver's license records by enacting the Driver's Privacy Protection Act of 1995, which directs the disclosure and sale of personal data contained in the records of state motor vehicle department. This Act applies to States and private individuals, and forces punishments for neglecting to conform to its requirements. Likewise the 'Computer Fraud and Abuse Act' forces criminal punishments on people who purposely get access to a computer without authorization, purposefully acquire information from a financial institutions or the government, with the intention to carry out a fraud and therefore cause damage. However, the Act is restricted in its scope and application rendering it an ineffectual method for combating the widespread abuse of data and the events of privacy crimes,

[13] Gaurav Goyal, *The Right to Privacy in India: Concept & Evolution* 67 (Partridge Publication, New Delhi, 2016)
[14] Nicole M. Buba, *The Right to privacy & Data Protection laws* 98 (Princeton University, New York , 2005)

 ISSN: 2582-6433

for example, identity theft.[15]

Further, the Electronic Communications Privacy Act of 1988 forbids the unapproved interference and disclosure or access to electronic communication services and for intentionally uncovering the content of such communication while in storage.[16] The prohibition relates with any electronic communication, for example, phone discussion or email, or even of any discussion in which the members show's a desire that such communication is no subject to interruption under conditions defending such a desire. Moreover, the 'Fair Credit Reporting Act' controls the accumulation and utilization of individual's information controlled by credit reporting agencies. Recent enactment passed by congress explicitly addressing to identity theft is the 'Identity Theft and Assumption Deterrence Act of 1997.'[17] This Act explicitly condemns the identity theft, and characterizes private citizens as direct victims of such conduct. Criminal liability for identity theft is forced on a person who intentionally transfers or uses, without legal authorities, a methods for identification of someone else with the aim to commit, or to aid or abet, any unlawful action that comprises an infringement of government law or that establishes a lawful offense under any state or local law. In addition to this enactment the Identity Theft Prevention Act of 2000 was presented in the U.S senate on March 2000.[18] The Act's expressed purpose for existence is to prevent identity fraud in consumer credit transactions and credit reports, and for other purposes. The bill would revise the Social Security Act to expose an individual to civil monetary penalty for falsely utilizing or selling a government managed social security number not belonging to that individual. Once more, such enactment does not adequately manage the issue of the easy accessibility of individual's information on the web. Hence, most of the federal states do not tackle the privacy issues introduced by the internet because they only administer the disclosure of personal recognizable information, and not the gathering or use of such information. Federal law, although recognizing and addressing the fact that issue of identity theft, is inadequate to manage with the strategies used by culprits to assemble the confidential data. In this manner, it is extensively certain that neither the current nor the proposed laws are adequate to manage or control these systems in the America and there is a need of powerful and achievable privacy protection laws.

On the other hand, the European Union has made a noteworthy step toward securing citizen's personal data. The European Union adopted the Data Privacy Directive, which is a far

[15] *Ibid.*
[16] Govind Mishra "Privacy and the Indian Legal System", 12 DLR 63- 64 (1990)
[17] Hyman Gross, "Privacy its Legal Protection", 41 EPW 23 (1976)
[18] K.K. Mathew, Democracy, equality and Freedom 89 (Central Book Publishing, New Delhi, 1st edn., 1978)

 ISSN: 2582-6433

reaching mandate administering the collection and use of personal recognizable information. Article.1 of the Directive sets out the goal that the member states will ensure the essential rights and freedoms of common people, and specifically their rights to privacy with respect to the processing of individual information. Thus, the order promptly and expressly recognizes a right to privacy.[19]

In England the Justice Committee inspected the entire subject of privacy.[20] The Committee proposed thorough enactment on the civil side, and prescribed that to utilize electronic, optical or other counterfeit gadgets as methods for secret surveillance ought to be made as a criminal offense to except from in certain defined conditions. The Committee likewise prescribed further investigation as regards criminal sanctions for industrial secret activities. Again the subject was analyzed by Younger Committee and in some cases they prescribed that there should be enactment to create either new offense so as to manage the new threats to privacy, for example new specialized technical surveillance gadgets; or a right of access by a person to data held about him by an assessment office. In other cases they felt that more viable authoritative controls would give better protection of privacy. India till date does not have an appropriate information insurance law. In year 2000, the government passed the Information Technology Act, a set of laws proposed to give a comprehensive administrative environment to electronic trade/electronic commerce. The Act additionally addresses computer crimes, hacking, and damage of computer source code, breach of secrecy and viewing of adult content.

Chapter X of the Act makes a Cyber Appellate Tribunal to settle the Cyber crimes, for example, damage to computer system under section 43 and breach of confidentiality and privacy under section 72 of the Act. At the time of enacting the Cyber laws for India, Parliament seems to have to a great extent disregarded the issue of privacy of personally identifiable data[21]. Section 72 of the I.T Act, is the only provision managing the matters is narrow in its scope. Save as generally given in this Act or some other law for time being in force, any individual, who in pursuance of any of the powers presented under this Act,[22] rules or regulations made there under, has verified access to any electronic record, book, register, correspondence, information, archive or document or other material without the assent of the person concerned, reveals such electronic record, book, register, correspondence, information, report or document or other material to some

[19] David M.O. Brien, *Privacy Law and Public Policy* 90 (Praegor Publishers, America ,1979)
[20] Govind Mishra, *Right to privacy in India* 45 (Preeti Publishers, New Delhi, 1994)
[21] *Supra note 16 at p. 6*
[22] Nandan Kamath, "A Guide to Cyber Law" , 34 JILI 98 (2008)

 ISSN: 2582-6433

other individual will be punished with imprisonment for a term which may extend upto two years, or with fine which may extend upto one lakh rupees or with both. Along these, it recommends a punishment for breach of privacy of any electronic record, yet applies just to offenses by authorities etc. Accordingly, there exists tremendous gap between the privacy needs of people and existing legislative protections in India. In fact, protection has been legislatively confined by the provisions in the Information Technology Act, the Telegraph Act of 1885 and the proposed Communications Convergence bill.[23]

Up to this point, the entire data protection disclosure and the effort to build privacy regulations in India, has occurred just with the regards to hold India's gigantic potential for business process outsourcing. There has not yet been any wider discussion surrounding the privacy implications of the government's collection, maintenance and use of personal information. For historical and cultural reasons, the objectives of the government in taking care of person's information are not suspected. Hence, a thorough privacy law is urgently required, not only to defend India's economic interests, but equally, if not more important, to protect the privacy of its citizens against the increasing destructive forces of the government. Till date the parliament has not enacted any law relating to privacy. It remains to be seen what would be the conditions to restrict it.

The privacy and information protection needs that the data about the people ought not to be consequently made accessible to different people and organizations. Every individual must be able to practice a considerable level of control over that information and its use. Data protection is lawful shield to prevent the abuse of data about different individuals on a medium including computer's. It is adoption of administrative, technical, or physical deterrents to protect individual's personal information. Privacy is firmly associated with data protection.[24] A person's information like his name, address, phone numbers, profession, family, likes and dislikes, etc are regularly accessible at different places like schools, universities, banks, directories, surveys and on different websites. Passing of such data to interested individuals can lead to intrusion of privacy like endless marketing calls. The primary principles on privacy and data protection specified under the Information Technology Amendment Act, 2008 are characterizing data, civil and criminal liability if there is any breach of data protection and infringement of confidentiality

[23] *Supra note 20 at p. 7*
[24] R.K. Suri, "Information Technology Laws law relating to cyber and E-Commerce", 87 JILI 89 (2000)

 ISSN: 2582-6433

and privacy.[25]

The Information Technology Act which came into force in the year 2000 is the main Act till date which covers the key issues of data protection, yet not every issue. Truth be told, the Information Technology Amendment Act, 2008 instituted by the Indian Parliament is the first enactment, which contains provisions on data protection. As indicated by section 2(1)(o) of the Act, Data signifies a portrayal of information, knowledge, facts, ideas or instructions which are being prepared or have been set up in a formalized way, and is planned to be handled or is being prepared or has been prepared in a computer system or computer network, and might be in any form including the computer printouts, magnetic or optical storage media, punched cards, punched tapes, stored in the memory of the computer.[26]

The Information Technology Act doesn't provide any meaning of personal data and, the meaning of the term 'Data' would be more significant in the field of Cyber-crime. Further, the IT Act characterizes certain key terms regarding data protection, like access, Computer, Computer network, Computer resource, Computer system, Computer database, Data, Electronic form, Electronic record, Information, Intermediary, Secure system, and Security procedure. The thought behind the aforesaid section is that the individual who has verified access to any such data will not exploit it by unveiling it to the outsider without acquiring the assent of the concerned party. 'Third party information' is characterized to signify 'any data managed by a mediator in his ability as a intermediary', and it might be doubtful that this limitation likewise applies to 'data' and 'communication'. Section 79 gives that an intermediary will not be liable for any third party information, data, or communication link made accessible or wished by him with the exception of the conditions gave in sub-Section (2) and (3) thereof.[27]

1.2 STATEMENT OF PROBLEM

The researcher chooses this topic because of the long interest in the topic of privacy and its protection. Information surrounds us and is created in about in all that we do. One sort is data that we may purposely share, and the other kind is the data which is delivered genuinely every time we achieve something paying little care to whether it is travel, a feast or using transportation. There is no burden that this information is enormously gainful and a few substances are glad to

[25] Information (Amendment) Technology Act , 2008, s. 2
[26] S.P. Sathe, Right to Information 34 (Lexis Nexis, Butterworth's, New Delhi, 2005)
[27] SV Joga Rao, *Cyber crime and Information Technology* Law 78 (Central Book Publishing, New Delhi, 2007)

 ISSN: 2582-6433

pay for access to this information. In reality, in this period of all inclusive and for all purposes free access to the web, information is the new money. It is significantly increasingly fascinating that the most extreme limit of information is till now not known. As innovation advances, more up to date applications are developed upgrading the estimation of data. The Researcher wants to find out the answer to the following questions:

- What data is?
- Who possesses it?
- Who accesses it?
- Why data needs protection?
- Which specific data needs protection?

Although, the data in today's scenario is intruded by both the state and non-state actors; So, the Researcher wants to pose answer to the primary problem of setting up of limits for both government and non-government agencies within which they can have access to the data of an individual. Governing bodies and Courts are overseeing the protection of data as a feature appropriate to protect and attempting to portray its degree and limitations.

Till today, India does not have a law to manage issues relating to safeguard or data protection. The current enactment i.e. the IT Act, 2000 and rules made there under, that touch the subject, are regional in nature and don't give an wide scope to various Articles i.e. Article 14, Article 19 and Article 21. The Researcher analyses how the judgment which is prominently marked as the "Privacy Case" or "*J. K.S.Puttaswamy (Retd.) v. Union of India and Ors.*[28]" will effectively affect the laws and regulations of India.

As, in 2017 under the Ministry of Electronics and Information Technology, Government of India had established a board of trustees of specialists committee under the chairmanship of a retired judge of the Supreme Court, Justice B N Srikrishna, to look at and propose changes to the data protection routine in India, the researcher will also analyse the recommendations of this committee and how these recommendations will enhance the subject of data protection by

[28] (2015) 8 SCC 735

 ISSN: 2582-6433

advancing the laws for this vary purpose. The Committee distributed a white paper on the data protection system proposed for India and welcomed open remarks on the equivalent. The Personal Data Protection Bill, 2018 a 'Draft Bill' had been proposed after discussions and consultations by the Committee. The draft bill is to a great extent encouraged by the European Union's General Data Protection Regulation, which came into force on May 2018. The draft bill provides an organized usage of its arrangements for more than a year and half after authorizing it. The problems in this 'Draft Bill' are also discussed in this research.

1.3 OBJECTIVE OF THE STUDY

The right to privacy has been brought into distinct quality in the legal writings in view of the fruitful debate among the lawful scholars and Judges. However, very scarce systematically recorded information as a book on legal aspect of privacy is available. The problem is further aggravated on account of the absence of a particular law and organizational guidelines guaranteeing privacy and secrecy. Subsequently, to make a broad and exhaustive investigation of the subject, this research is proposed to be embraced in view of the following objectives in mind:

1. To discover the systematic evolution of privacy with special reference to data protection in India.
2. To investigate the legal provisions of the Indian legal framework and to recognize and highlight the constitutional position of this right under our Constitution especially Part III dealing with the Fundamental Rights.
3. To focus on the emerging difficulties of new technological age, a social change and to point attention towards how and to what degree the legal framework has adapted the further extension and protection of the right to privacy.
4. The focus of this study would be to make available the perspectives of the Judges specifically cases as an impression of legal frame of mind towards privacy as a right and how and why and to what extent it is to be ensured against invasions or intrusions. This would include a basic assessment of judicial reaction in encouraging and furtherance of this right.

1.4 HYPOTHESIS

The research proceeds on the listed hypothesis:

 ISSN: 2582-6433

a) Right to privacy is ought to be incorporated into Part III of the Constitution of India in order to give express constitutional acknowledgment to this right as one of the fundamental rights.
b) There is a need to guard the privacy right from the risk of intrusion radiating from contemporary technological advancements.

1.5 REVIEW OF LITERATURE

The study on the "protection of privacy in India" has been attempted by the various researchers of the diverse background. However, several studies have been conducted on right to privacy in India examining the nature, extent and magnitude of the problem. In this context how different studies has tackled the various dimensions of the problem of protection of privacy in India will be examined in the review of the literature as follows:

Books Referred As

Hyman Gross[29] in his book "privacy: its legal protection" has laid down that privacy cannot exist at all without protection. Bare physical intrusion of private things cannot be secure in private places; all measures to provide safeguards for their communication or disclosure are pointless. In society there are two interests i.e. making privacy secure is one and making lives proper is another interest. There should be a balance between these two interests for the smooth functioning of the society.

K.K. Mathew[30] in his book "Democracy, equality and freedom" laid down that, Exercise of the right to express oneself might in certain circumstances come into conflict with those interests of other individuals right to privacy i.e. the right of a person to be free at some point from intrusion by society into his intimate and personal affairs. There should be proper balance between the life of a person as an individual and his life as a member of society

David M.O. Brein[31] in his book "privacy law and public policy" revealed logical Fallacies and failure to account for various kinds of privacy interest and litigation. Right of privacy is a product of social structure, conventions and legal policy. Moreover such right does not include when and how one will have privacy? Therefore in order to eradicate the legal

[29] Hyman Gross, *Privacy its legal protection*, 122 (Oxford University Press, London, 1976)
[30] K.K. Mathew, *Democracy, equality and Freedom* 56 (Eastern Book Publishing, New Delhi, 1978)
[31] David M.O Brien, *Privacy Law and Public Policy* 64 (Praegor Publishers, America, 1979)

 ISSN: 2582-6433

boundaries of privacy, an alternative analysis of privacy must construct a framework that does not confuse privacy and the right of privacy.

Paul O Higgins[32] in his book "Cases and materials on civil liberties" agreed that concept of privacy embodies value which are essential to the working of a free society. Any general civil remedy would require hardly a less general qualification in order to enable the court to achieve an acceptable balance between values implicit in respect for privacy and other values of at least equal importance in a free society of the open circulation of true information.

Govind Mishra[33] in his book "Right to privacy in India" examines critically and thoroughly the given by the scholars and judges in India to the constitutional aspect of the right to privacy. He throws light on the recognition of privacy in the legal and moral norms of ancient Indian society and traces the recognition of the right to privacy in the customary and statutory laws of British and contemporary India.

S.K. Sharma[34] in his book "Privacy laws: A comparative study", had attempted to express privacy in national and international perspective. He states that privacy is a guarantor of individual's moral autonomy which is a basic value in a democratic system of government. Privacy can be defined as a right to control one's information and one's physical being. Both rights are closely related to the principle of respect for person. Both must be reinterpreted in the light of technological context.

D.D.Basu[35] in his book, "Law of the Press", is of the view that privacy is a recent development in the realm of law and the stream of its development is still flowing. It is very difficult to give an extensive definition of what privacy means in law. Loosely it has described as the right of a person to be 'let alone' or his right of repose in his private life and home.

Nandan Kamath[36] in his book "A Guide to cyber laws", laid down the personal data privacy in online context. According to him the essence of the privacy of the personal data is the understanding that individual can legitimately claim that data about themselves. Privacy is the

[32] Paul O. Higgins, *Cases and Materials on Civil liberties* (Sweet & Max well, London, 1980)
[33] Govind Mishra, *Right to Privacy in India* (Preeti Publication, New Delhi,1994)
[34] S.K. Sharma, *Privacy Law: A Comparative Study* (Atlantic publisher, New Delhi, 1994)
[35] D.D. Basu, *Law of the Press* (Universal Law Publishing, New Delhi, 2002)
[36] Nandan Kamath, *A Guide to Cyber Law* (Central Book Publishing, New Delhi, 2008)

 ISSN: 2582-6433

interest that individuals have in sustaining a 'personal space' frees from interference by other people and organizations.

Parag Diwan,[37] in their book, "Information technology laws, laws relating to cyber and e-commerce", laid down the classic definition of the privacy concept that it consists of the right to be let alone in terms of isolation from the scrutiny of others.

John Bennett [38] in his book, "Policy instruments in global perspective", offers a broad and incisive analysis of the governance of privacy protection with regard to personal information in contemporary advanced industrial states. Based on research across many countries, it discusses the goals of privacy protection policy and the changing discourse surrounding the privacy issue, concerning risks, trust and values.

Mashood A. Baderin[39] in his book, "International Human Rights and Islamic Law", laid down the right to privacy in Islam, the right to privacy is also generally well stressed under Islamic law. The shariah prohibits any unlawful intrusion into the private life. Specific aspect of privacy addressed by the Human Rights Commission includes family home, correspondence honour and reputation etc.

S.P. Sathe[40] in his book, "Right to Information", laid down that the right to freedom of speech and expression often collides with the two rival rights namely 'right to privacy' and 'right to fair administration of justice'. Both the rights are protected by the law of torts and contempt of court respectively.

S.V. Joga Rao[41] in his book, "Law of Cyber Crimes and Information Technology Law", laid down that major human rights concern in the cyber space is the threat to individual is likely to increase rather than decrease. Regional bodies such as the Commission of the European Union have attempted to uphold privacy principles by limiting the transfer of personal data to countries, which do not offer comprehensive and effective National Laws for the protection of privacy.

M.P. Jain[42] in his book, "Constitutional Law"; which have been concerned with the

[37] Parag Diwan, *Information Technology Laws relating to Cyber and E-Commerce* (Allahabad Book Agency, Allahabad, 2000)
[38] Colin John Bennett , *Policy Instruments in Global Perspective* (Princeton University Press, New York, 2003)
[39] Mashood A. Baderin, *International Human Rights and Islamic Law* (Eastern Book Company, New Delhi, 2003)
[40] S.P. Sathe, *Right to information* (Atlantic Publishing, New Delhi, 2005)
[41] S.V Joga Rao, *Cyber Crime and Information Technology Law* (Universal Law Publishing, New Delhi, 2007)
[42] M.P. Jain, *Constitutional Law* (Wadhwa & Company, Nagpur, 2007)

 ISSN: 2582-6433

several developments that have taken place in the region of the Indian constitutional law. Some of the judicial pronouncements are very significant and turning point in the constitutional law. The Hon'ble Supreme Court of India has been displaying a very creative and activist streak. Article 21, has been given a completely new orientation. The court has implied a bundle of rights for the people from Article 21 such as right to privacy etc.

Ajay Dash[43] in his book, "Sting operation by media", tries to bring out the hidden secret of the sting he tried to prevent the intricacies associated with the skilful tactics in a very lucid manner, taken in to account the right to privacy, he comment that the right to privacy and public right to know are often cast as opposite but both are vital in a modern democracy, freedom of media is essential in maintaining on informed, confident and prosperous nation. A right to privacy is essential in preserving our dignity.

Prof. Narendra Kumar[44] in his book, "Constitutional law of India", has attempted to express complicated ideas with clarity and accuracy. His work incorporates all the important judgements of Apex Court and the High Court related to privacy law in India.

James. B. Rule[45] in his book, "Global Privacy protection", traces the birth and early history of privacy, and the need for its protection as a public issue. He focuses on controversies over the fate of personal data held by the government and private institutions in conventional or computerised files. He laid down what forms of privacy protection were readily accepted in each country and which were contested what different government agencies did and did not define roles for themselves in protecting people's interest in treatment of their data.

Hariom Marath[46] in his book, "Justice delayed is Justice denied", attempted to lay down the laws relating to privacy. He laid down the intrusion into privacy may be by legislative provisions, administrative orders and by Judicial orders. The legislative intrusion must be tested on the touch stone of reasonableness as guaranteed by the constitution and for that purpose the court can go into the proportionality of the intrusion.

J.N. Pandey[47] in his book, "Constitutional law of India", 54thedition of the book has been

[43] Ajay Dash, *Sting Operation by Media* (Eastern Book Company, New Delhi, 2007)
[44] Prof. Narendra Kumar, *Constitutional law* (Allahabad Law Agency, Allahabad, 2008)
[45] James B. Rule, *Global Privacy Protection* (Edward Elgar University Press, America, 2008)
[46] Hariom Marath, *Justice Delayed is Justice Denied* (Lexis Nexis, Butterworths, Nagpur, 2008)
[47] J.N. Pandey, Constitutional Law of India (Central Book Publishing, New Delhi, 2017)

 ISSN: 2582-6433

brought up to date by incorporating all the constitutional developments and judicial decisions relating to the several aspects of the privacy protection in India.

Articles Referred As

The Economic Laws Practice (journal)[48] in their article "Data protection and Privacy issues in India" defined privacy as "Privacy is the right to be left alone or to be free from the misuse or abuse of one's personality. The right of privacy is the right to be free from unwarranted publicity, to live a life of seclusion, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned".

Sindhu balaji[49] in her article stated that, "India is one step closer to having its own data protection law after the Srikrishna Committee submitted its initial assessment and recommendations on data privacy and management last week in a 176-page report, as well a draft of the legislation on data protection titled Personal Data Protection Bill, 2018. Even as the recommendations continue to stir debate, technology companies, start-ups and industry bodies are united in their stance for a law that should safeguard customers and help accelerate India's fast growing digital economy".

Eleni Kosta[50] in her article "Data Protection issues: Pertaining to social networking" discusses how the implementation of current communication methods promotes effective exchange of information and cooperation between different actors on social media services and also how social media network fits into the current European data security regulatory framework. The author also explores certain particular problems related to information security, concentrating on the position of both the appropriate performers, using the instance of picture uploading, social media use and online safety, etc.

Kamlesh Bajaj[51] in his article "Data protection- security and privacy" discuss the globalization's effect on identification privacy is increasing. The idea that more private information crosses boundaries in inter-border data transfers implies that violations of data

[48] Available at: https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf (visited on 17/6/2019)
[49] Available at: https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#4cc664a070fe (visited on 17/6/2019).
[50] Eleni kosta, "Data Protection Issues: Pertaining To Social Networking" 26 EPW 89 (2010)
[51] Availableathttps://www.dsci.in/sites/default/files/documents/resource_centre/Privacy%20and%20%20Data%20Protection.pdf (Visited on 17/6/2019)

 ISSN: 2582-6433

frequently influence individuals in various nations and can lead to economic corruption. These crimes must be dealt with in the laws of public data security. To guarantee information security, a powerful data privacy system needs coverage of computer crimes of all types. The modified IT Act does specifically as it has attempted to react in a manner that amplifies the faith of the current cyber space.

Jayant Das[52] in his article "Increasing Intrusion of State into Right to Privacy" discusses how state intrudes into an individual's privacy by means of enacting laws such as Aadhaar Act etc. The author also analysed the leading cases including the Puttaswamy case and it's important findings and its impact on the parliament.

1.6 RESEARCH METHODOLOGY

The research methodology for the study is doctrinal in nature & the research is a descriptive and explanatory in nature. This study is adapting the historical approach and based on the documents and published materials which are important to the present research. The study is based on the examination of the Constitutional law and the statutory provisions related to Right to Privacy and Data Protection Law's. This research has focus on both primary and the secondary Data. The source of the research is secondary in nature. All the material has been collected from the authoritative publications and has been help with the cases from the journals. The descriptive method is used to examine the interpretation and treaties on the international related to the Privacy and Data Protection in the constitution. The research is systematic search for the relevant information on the topic. A research design is systematic planning for the proper research in present context.

1.7 SIGNIFICANCE OF STUDY

The common proverb that' information is power' also seems to have different implications for the person's actions for which data is immensely powerful, even a wide sweeping range. Information is rapidly monitoring financial, social and political control. Information is used to communicate about transactions and resources; political control is grouped and modified depending on data, and even human interactions and relations are described in personal data trading. This makes the collection of data by the officials more ensured and especially the

[52] Available at https://www.dailypioneer.com/2018/state-editions/increasing-intrusion-of-state-into-right-to-privacy.html (Visited on 18/6/2019)

 ISSN: 2582-6433

protection of data of fundamental importance[53].

The abuse of individual information is equally wrong with essential safety. At the stage where data is collected for one purpose and subsequently handled in an unpredictable manner, a recognizable harm is established by the failure to fulfill the first desire. Protection of information shows a absurd debate and principle display. The conversation often brings together a broad range of interests and characteristics. Security doesn't match completely into a calculated single model. Informative liberties characterize the work of a resident in the processing of personal information. There is this, and much more to speak, conventional depiction and practice, that would end up with the need for data protection laws in the Indian background.

Through the privacy judgement, the Indian Supreme Court featured how "the risk to data security can begin from both the state and non-state components as well" and instructed the government to develop a strong cyber security plan accordingly. In addition, the Court considered, along these lines, the way in which information security was undoubtedly a complex exercise that the State should have adopted after an equalization of privacy issues and actual state interests. The result would probably be a law that considers breach of information privacy to be recognizable and non-bailable offense.

1.8 CHAPERTISATION PLAN

The researcher has conducted the following research regarding the “Right to Privacy and Data Protection Issues: A Critical Study with Reference to Indian Perspective” under the following chapterisation plan:

1. Introduction
2. Right to Privacy and Data Protection in General
3. Legal Frameworks Relating to Privacy and Data Protection in India
4. Socio-Legal Effects of The Data Protection
5. Judicial Approaches Towards Right to Privacy & Data Protection Laws in India
6. Conclusions and Suggestions

[53] *Supra note at 18 at p. 7*

 ISSN: 2582-6433

- **Chapter One: Introduction**

In this chapter, the researcher includes the introduction, research methodology, literature review, hypothesis, significance of the Right to Privacy and Data protection in India. He has also studied the objectives behind the research conducted on the Privacy Right and Data Protection in India. This chapter includes the general overview to the concept of privacy right as an essential right of the citizens and also the problem faced by this right in today's era of information and data.

- **Chapter Two: Right To Privacy and Data Protection in General**

In the second chapter the researcher has included the general overview of the Right to Privacy and Data Protection. The chapter includes the elaborative explanation of the concept of privacy and some dictionary and scholarly definitions of privacy right. The chapter includes the root or the origin of the privacy right and its development in different times. Privacy and its presence in different dimensions are also included in this chapter.

- **Chapter Three: Legal Framework Relating to Privacy and Aadhaar Act, 2016**

In the third chapter the researcher talks about the law's presently operating in India in regard to the privacy and the data protection. The chapter includes all the constitutional provisions which are considered to be connected to the privacy specifically Article 19 and Article 21. All the different legislations like Information Technology Act, Hindu Marriage Act, Indian Penal Code, Indian Easement Act, Copyright Act, Children Act, Credit Information Companies (regulations) Act, Right to Information Act, Evidence Act and many more are also included in this chapter. The researcher also included in this chapter several schemes like 'Unique Identification Scheme' and 'NPR Scheme'. Moreover the chapter also includes the expert committee's recommendations and the Draft Bills relating to Data Protection.

- **Chapter Four: Judicial Approach**

In the four chapter, the researcher focuses on the approach regarding the right to privacy and protection of data, followed by the judiciary. This chapter deals with the various case laws which reflect the attitude of the Indian judicial system about the privacy rights in the

 ISSN: 2582-6433

Indian society. It also analyzes the recent development towards the privacy as a fundamental right. And it also talks about present threat in the protection of data in this cyber society. This chapter shows the efforts taken by apex court to prohibit the breach of the right to privacy to maintain the essence of the constitution in the country.

- **Chapter five: Conclusion & Suggestions**

In the Last chapter, the researcher finally concluding the topic by giving various suggestions to the concept of Right to Privacy and Data protection in the country and also throw light on the present scenario followed by the society and its impact on the modern society. It also describe the following recommendation so that to improve the condition in the India and also to adopt the firm and efficient legal framework so that to achieve the goal to provide protection of data from any kind of mishappening.

CHAPTER-TWO

RIGHT TO PRIVACY AND DATA PROTECTION IN GENERAL

"Every breath you take and every smile you fake, every move you make and every step you take,

 ISSN: 2582-6433

every claim you stake and every vow you break, 1'11 be watching you".[54]

- Disgruntled Lover

2.1 INTRODUCTION

The concept of privacy is not old in India. The ancient Indian knowledge theory, based on all literature from Upanishad, prescribes meditation, which must be done without any external disruption. The estates and the 'Arthashastra' show sufficient concern and regard for the privacy of the individual. The use of curtains is defined in the Ramayana and other classical literatures are developed in a certain manner.

Private life is the thing that everybody needs to limit to him and other feel crazy in earthing the same. It is this private life which improves or decreases or in other words shapes the public life. Your commitment to the world would be a nullity, regardless of what endeavours and devotion you may have put for public, if you carry an awful private life-be it living in luxury with assets which are in excess of your known income or you are found spending night somewhere else. So, you are constantly under investigation for a life which is yours-own, personal and valuable, and in this manner you can conclude that there is no privacy. During the laissez-faire period, a person's relation with the government was inconsiderable. Yet, in a modern administrative state, one needs to manage the administration in practically different backgrounds. The separation between the public life and private life of an individual has diminished. At whatever point an individual enters into a relation with the administration he needs to present a ton of personal information. In specific cases the government itself may gather data with respect to people.[55] Data about individuals might be important for an administration for framing its policies in a democratic way[56]. The surveillance by government over its citizens is a key method for social control. When it gives welfare benefits, the administration may need to probe deep into society and accumulate data. Accumulation of Personal data becomes important additionally to scold present day organized criminals. People working in departments of the military section, foreign affairs and nuclear energy may have be watched by the administrations.

This procedure of data gathering definitely affects the privacy of the individual yet such

[54] Suvendukumar Pati, "Right to Privacy -Whether Fundamental?" 27 IBR 151 (2000)
[55] M.C. Pramodan, "Right to Privacy" 14 CULR 6 (1990)
[56] *Ibid.*

 ISSN: 2582-6433

a procedure is regularly important for a productive working of government and especially when it is the national interest. But in such case, there ought to be a guarantee that the governmental authorities uses such personal information just for the official purposes for which they are required.

The right to privacy is natural and inalienable in any social order however, its degree or depth may differ depending upon the way of life, culture, religion, scientific advancement and the political and legal systems. Anyway there is a hardcore of the individual data which be shielded from interruption and a hardcore of personal information which can be disclosed to the general public. The purpose behind such privacy and publicity is the public interest. In between them lies an adaptable part which might or might not possibly be secured under the head of rights to privacy depending upon a specific circumstance in a society.

Privacy is an idea identified with solitude, secrecy, and autonomy, however it isn't synonymous with these terms; for beyond the purely expressive aspect of privacy as isolation from the organization, the interest and the impact of others, privacy suggests a normative component: the right to exclusive control of access to private domain.

A right of privacy is recognized both in law and in common language, yet different legal systems emphasize distinctive perspectives, and traditions related with privacy vary significantly from culture to culture and from circumstance to circumstance. In a considerable amount of the claims to the rights to privacy are hard to distinguish from different claims to respect for the personal integrity, and from claims against interference by the government and other external agents.[57]

2.2 CONCEPT OF RIGHT TO PRIVACY

2.2.1 Definitions of Privacy

According to the Duhaime's Law Dictionary[58] the privacy means "An individual's Right to control and access over his/her personal information". This definition is a layman translation to what privacy in simple sense means. It simply indicates that privacy right of an individual is his/her full control and undisrupted access over his/her own personal information. The personal

[57] Arnold Simmel, "The Right to Privacy in India" 12 IESS 480 (1968)
[58] Available at http://www.duhaime.org/LegalDictionary/Category/CriminalLawDictionary.aspx (Visited on 22/ 6/ 2019)

 ISSN: 2582-6433

information here includes- his name, address, demographic data, his personal affairs, his private space etc.Gillian Black[59] in his book defines the privacy as "Privacy is a desire of an individual to be free from the other's intrusion". The definition states that every individual is having the right of enjoying his personal choices, his personal affairs free from the interference of other people into it.

European Convention on Human Rights in Article 8[60] defines the privacy as "Every individual have the Right to respect for his family and private life, his home and his correspondence". This is a huge effort by the Human Right Convention on the international level to define the importance of privacy in an individual's life. The Article further stated that no Governmental Agency is allowed to intervene the privacy right of a person until and unless, the said intrusion is in accordance to the law and is necessary for the purpose of security of the state, public wellbeing, and essential for the economical wellbeing of the country. Justice Cory of the Canadian Supreme Court in a case[61] defined privacy as "Privacy is the situation of being alone, in a case of preferences or freedoms, uninterrupted and independent of government scrutiny; safe from intervention or disturbance. The capacity to exclude anyone from the property is a significant element of privacy. A main aspect of privacy is the right to be free of intrusion or interference."

Privacy according to Justice Dickson[62] is "The freedom of a man to ascertain when, how and to what degree he or she will disclose private data, can be characterized as privacy. A sensible idea of privacy requires a person to continue on the belief that the State may only infringe this right by capturing personal communications on a hidden basis if it has determined to the satisfaction of a judicial officer that, an offense has been performed or is being performed and that monitoring of communications provides proof of the crime."

Indian scholar D.D Basu[63] in his book defined privacy as "Privacy is the recent development in the kingdom of law and the river of its development is still flowing. According to him it is very difficult define what privacy means in law. He states it simply means as the right of a individual to be 'let alone' or his right of repose in his private life and home."

[59] Gillian Black ,"*Publicity Rights"* 2 EPW 8 (2011)
[60] Availableathttps://www.jus.uio.no/lm/coe.convention.on.human.rights.1950.and.protocols.to.1966.consoloidated/landscape.letter.pdf (Visited on 22/ 6/ 2019)
[61] R v. Edward (1996) 1 SCR 128
[62] R v. Duarte (1990) 1 SCR 39
[63] D.D. Basu, *Law of the Press* 112 (Eastern Book Company, New Delhi, 2002)

 ISSN: 2582-6433

The Hon'ble Supreme Court of India in the case *J. K.S Puttaswamy v. Union of India*[64] held that "The privacy rights is guaranteed in accordance with Article 21 as an inherent component of the right to life and personal liberty and as portion of the rights provided by Part III of the Constitution."

2.2.2 Meaning of Privacy and its Definitions

The concept of Privacy is hard to define in light of the fact that it is vague and temporary, frequently meaning strikingly different things to different individuals. This is on the grounds that protection is a thought that is emotional in its appeal and grasps a large number of various rights, some of which are interwoven with others, often randomly or conflicting.

Privacy has been interpreted as the capacity of an individual or a group of individuals to keep their live and personal issues out of public's visibility, or to control the flow of data about themselves. Privacy is now and then related with secrecy despite the fact that it is usually highly valued by individuals who are publically known. The least difficult definition of privacy is given by Judge Cooley; he called it as "the right to be left alone".[65]

Recently, lawyers and social scientists have been achieving the conclusion that the fundamental quality of a successful right of privacy is the person's capacity to control the circulation of data relating with him, a power that often is basic to maintain the social relationship and individual's freedom correctively. When an individual is denied of command over the nozzle that regulates the flow of information relating to him in some measure he becomes subservient to those individuals and organizations that can control it or manipulate it. Custom-based law was surely, the first to portray this concept. As indicated by Justice Cooley, the right to respect for private life is this right to be let alone.

As indicated by an American court, it is correct to live on with one's life in isolation, without being exposed to undesired exposure. To put it short, it is, as Cooley stated, 'the right to be let alone'. The Restatement of the law of Torts sets out that an individual who unreasonably and genuinely interferes with other's interest for not having his affairs known to other people or his likeness displayed to the public is liable to the other. The assurance of privacy might be seen as having three aspects: spectators and intruders are to be kept out of the people private zone; the

[64] (2015) 8 SCC 735
[65] Dhruv Jain, "The Right to Privacy in India : An overview", 6 IHSS 37 (2006)

 ISSN: 2582-6433

individual isn't to be demanded an explanation from in regard of issues in which property belongs to his private sphere and the person whose privacy is intruded in either two ways is to have a lawful remedy against such intrusion.

The technological advancement and the expansion in the flow of information initiated by the computer threaten the person's capacity to control the flow of information about himself. At the end of the day, his privacy is endangered. The right to privacy is hard to define. A board on office of Science and Technology characterized it as pursues: The right to privacy is the right of the person to choose for, him the amount he will impart to others, his thoughts, his Feelings and the certainties of his personal life.[66]As a matter of fact what is Private, varies from day to day and setting to setting. The Panel perceived that privacy relies upon numerous components, the nature of the society and the specific conditions of the event.

Today the most difficult issue confronting man is 'information'. Truth be told, the technical and scientific gadgets made it simpler to accumulate private or public information and harder to control the utilization made of them. Data about an individual comprises a danger to the classified nature of his private life, his family and his home. Intrusion of privacy implies an unjustified misuse of one's identity or interruption into one's private movement, actionable under tort law and once in a while under Constitutional law.

Nordic Conference of Jurists in May 1967 gives a significantly more extensive definition of right to privacy. They concluded that, the right to privacy implies, the right of the person to lead his life protected against:

- Interference with his private, family and home life.
- Interference with his physical or mental integrity or his moral or intellectual freedom.
- Attacks on his respect or reputation.
- Being placed in a false light.
- The revelation of immaterial embarrassing actualities related to his private life, the utilization of his name, identity or resemblance.

[66] *Supra note 63 at p. 25*

 ISSN: 2582-6433

- Spying, prying, watching and plaguing.
- Interference with his correspondence.
- Misuse of his private communications, written or oral.
- Disclosure of data given or received by him in conditions of professional confidence.

2.3 DIFFERENT DIMENSIONS OF PRIVACY

There are numerous dimensions to the Right to Privacy. They are followings:

2.3.1 Political Privacy

It may sound like an odd thing to say but with an ever increasing amount of people in today's globe. The e-campaigning is the future for net consumers. Vast amounts of data can be collected through cookies, internet donation forms, etc. as to which candidate which the voters prefers, which sites he surf, etc[67].

2.3.2 Medical Privacy

Information about a person's health is held secret and the sick person must give his approval in most nations before it could be shown to anyone except hospital employees. In some instances, however, failure to reveal one's health condition may be unlawful. With the rise in the amount of medical developments such as brain mapping, DNA testing distinctive to each human; medical privacy is being heatedly debated.[68]

2.3.3 Genetic Privacy

Our vocabulary has only recently joined the term "genetic privacy" it is to avoid genetic discrimination based on obvious or suspected genetic disorders. It is essential as, because of individual's family history of a specific genetic disorder, an individual may be fired from his work or may lose his colleagues etc., whether or not he is infected doesn't matter. Genetic privacy

[67] Javed Alam, *Privacy & Data Protection Laws in India* 23 (Asian Book Publishing, New Delhi, 2016)
[68] Dhruv Jain, *Right to Privacy Laws In India* 37 (Universal Law Publishing, New Delhi, 2007)

 ISSN: 2582-6433

is therefore very essential to protect the interest of such individual's[69].

2.3.4 Internet Privacy

Using the Worldwide web leaves a trail of user information unless you use privacy software or a proxy server. History, cache or archives of a web browser could be obtained to expose what the person did. In addition, the visited domains already have their own archives indicating each computer's IP addresses and other information to which they offer connections. In addition to this, there are other aspects of privacy i.e. during internet career search, corporate privacy, government intrusion privacy, etc.

2.4 ORIGIN OF RIGHT TO PRIVACY

Privacy is something which nearly everybody in the world cherishes. It is the freedom to live life in which we have a right to be let alone and without the govt. Privacy enables us to evolve as an individual with our own ideas, opinions, hopes and aspirations. It allows us to establish in our own dwellings the rules that how to live our own lives. Privacy enables adolescents to judge who they should wed, whether they should have babies, and how to raise families. The right to privacy prevents our lives to be investigated by the state.The phrases "privacy" and "right to privacy" do not, surprisingly, occur in the United States Constitution. Rather than, some parts of the Constitution safeguard particular types of privacy. For instance, the First Amendment to the constitution i.e. freedom of expression and religion, guarantee the right to personal thoughts and ideas. The Fourth Amendment states that without excellent purposes, the state may not seize a individual or inspect his home. The Fifth Amendment provides, there is no need for a convicted person to witness at court against himself. That implies any data about the crime he is charged with can be kept confidential.

2.4.1 Developing the Right of Privacy

Boston attorneys named Louis D. Brandeis and Samuel D. Warren were the first Americans to mention the right to privacy. They released an essay called "The Right to Privacy" in 1890. Brandeis and Warren said American's require security from the newspapers that breached privacy by revealing the audience to personal and professional life. Papers frequently wrote insulting or offensive columns about the people. Brandeis and Warren said American

[69] *Ibid.*

 ISSN: 2582-6433

citizens should have the right to prosecute news papers in order to safeguard their privacy.

Brandeis became a Justice of a U.S. High court in 1916. He authored a renowned dissenting opinion twelve years later in Olmstead v. United States and said that the Constitution was designed to safeguard privacy to aid Americans embrace joy: "Our Constitution's makers in their views, ideas, beliefs and emotions, they attempted to safeguard American people. They are given the right to be let alone, the most extensive of human rights, and the most appreciated right by civilized men, as against state."[70] Nearly four more decades passed before a particular right of privacy was acknowledged by the Supreme Court. In the meantime, some judges wrote views that supported such a right. In *Public Utilities Commission v. Polla*[71], Justice William O. Douglas said "the right to be let alone is the start of all liberties." Also in *Poe v. Ulman*[72], Justice John Marshall Harlan II referred to Connecticut law which interfered in marriage as "an unbearable invasion of privacy."

In *Griswold v. Connecticut*[73] , a right to privacy in the Constitution of United States was finally acknowledged by the Supreme Court. The situation engaged a Connecticut act that held any use of contraceptive methods or birth control unlawful for married couples. Nothing explicitly in the Constitution says that married couples are permitted to use birth control. However, the Court said that the legislation clashed with "the right to privacy in marriage." In other terms, privacy in America enables married people to decide whether to use contraceptives or not. The Court had to decide since Griswold what the privacy right protects. In cases concerning marriage, sexual reproduction, abortion, marriage and family, the right to die, and the right to keep data confidential, the problem occurs. In these cases, the Supreme Court sometimes recognizes the right to privacy, but in other it does not.

2.4.1.1 MARRIAGE

As Griswold pointed out, marriage is one of the privacy-protected relationships. That's because families are a major component of American lifestyle. Individuals who are often grow up dreaming of having their own family one the day. One way for Americans to seek joy in life is to settle with a family.

[70] (1928) 277 U.S. 438
[71] (1952) 343 U.S. 451
[72] (1961) 367 U.S. 497
[73] (1965) 381 U.S. 479

 ISSN: 2582-6433

Therefore, many incidents of privacy related to the family took place. For example, two years after Griswold, the Supreme court ruled in case *Loving v. Virginia*[74] had a Virginia law that made it unlawful for people of different races to marry one another. The Lovings were a white man and a black woman and were found guilty under this law. The Lovings made an appeal against their convictions and won. The Supreme Court ruled that marriage was one of the "basic civil rights of person."

Zablocki v. Redhail[75] and *Boddie v. Connecticut*[76] have been included in other marriage related instances. In zablocki, the Supreme Court said legislation that makes getting married to poor individuals financially difficult infringe the privacy rights. Rationally, there must also be the liberty to marry and to divorce. The Court then invoked laws in boddie that render getting a divorce financially hard for poor individuals.

2.4.1.2 Sexual reproduction

As marriage right is protected by privacy, it also protects the option to have kids or not. As mentioned above, the Griswold Court said that the state could not stop the use of contraceptive devices by married couples. The Court held in *Eisenstadt v. Baird*[77] that married couples have the right to use contraceptives for privacy reasons. Also in Carey v. Population Services International, the Court said that the state could not stop contraception from being used by individuals under the age of sixteen. These judgments, held together, protect the freedom of each American to decide whether or not to have kids.

Many individuals think that these decisions often safeguard the right of a couple to participate in sexual relationships, whether they attempt to have kids or not. Soon the issue appeared whether the privacy right provides protection o homosexual relationships. There are laws in many countries that simply make homosexual relations a crime.In *Bowers v. Hardwick*[78], the U.S. Supreme Court declared that legislation that declares homosexual relations a felony may not violate right to privacy. The Court said that the privacy right protects America's traditional relationship that implies a male and a female marriage, their family, and sexual reproduction.

[74] (1967) 338 U.S. 1
[75] (1968) 434 U.S. 374
[76] (1971) 401 U.S. 371
[77] (1972) 405 U.S. 438
[78] (1986) 478 U.S. 186

 ISSN: 2582-6433

2.4.1.3 Abortion

If privacy, by using birth control includes the right to prevent pregnancy, does it safeguard the right to stop pregnancy by getting an abortion? This is one of America's most heatedly discussed issues. Activists in abortion rights, claim that the women whose bodies are affected by pregnancy, have a constitutional right to have an abortion. They claim that women are given this right because of the consequences of the medical risks and long-term impact of having the baby. Abortion opposers, who claim that an unborn has a 'right to life' as a living individual, abortion is a killing for them.

The Supreme Court in *Roe v. Wade*[79] landmark decision held that privacy guarantees the right to have an abortion until the unborn can reside outside the womb of the mother. At that stage, by stopping abortion, the state can safeguard the life of the unborn unless it is essential to save the life of the mother. After Roe, individuals keep arguing about whether abortion should be legal or not.

2.4.1.4 Family life

People spend many years maintaining their families after they get married and have kids, trying to keep them as healthy, protected and comfortable as necessary. The right to privacy enables people to take many household decisions. For instance, the Supreme Court said in *Pierce v. Sisters*[80] Society that fathers do not have to send their children schools. As soon as parents assure good schooling for their children, they can send their children to private or government institutions or educate them at home.

Another family privacy situation was *Moore v. City of East Cleveland*[81]. East Cleveland had a law requiring individuals residing in a building to belong to one family. The law described a family as mother and father, as well as parents and children. By convicting Inez Moore, a lady who resided in a flat with her unmarried son and two siblings, Cleveland implemented the law. Moore said the law infringed her privacy right and the Supreme Court agreed with her. The Court said Americans are permitted to reside family with family outside the traditional "nuclear family" of mother, father, and children.

[79] (1977) 431 U.S. 494
[80] (1925) 268 U.S. 510
[81] (1977) 431 U.S. 494

 ISSN: 2582-6433

2.4.1.5 The Right to Die

The privacy right allows Americans to choose how to live. Is it protecting the right to die as well? If a individual has only six miserable months to live of cancer while dying, is she entitled to end her existence to prevent the pain? Can a family shut down somebody who will be in a coma for remainder of her life from the life support system?

The last question was the problem in Cr*uzan v. Director, Health Department of Missouri*[82]. Nancy Cruzan was alive after a car accident in 1983, but was unable to travel, talk, or communicate with almost no chance of healing. Believing Nancy didn't want to live like this, her parents chose to shut down her life support system. The state of Missouri did not allow that so the relatives of Nancy brought the case to the U.S. Supreme court. Although the Supreme Court ruled in favour of Missouri, it also said Americans are entitled to refuse undesired treatment, even if it will cause death. The right to privacy, in other terms, involves the right to die. Only when further proof came up that Nancy would never want to live in misery Nancy's family was permitted to remove the life support system.

2.4.1.6 Private Information

The start of the Information Age was at the end of the twentieth century. Computers store large quantities of individual's information. Americans are, of course, worried about the availability of personal data to the outsiders. They also fear that public officials trying to explore criminal activity will violate their privacy. At the same moment, to carry them to justice, the state requires to investigate and capture criminals.

To a specific degree, Americans are secured by the privacy laws. The Federal Omnibus Crime Control and Safe Streets Act of 1968 direct the administration's utilization of wiretapping to listen to phone conversations. The Privacy Protection Act of 1974 and the Freedom of Information Act require the administration to be reasonable when it gathers, utilizes, and discloses private information. Sometimes, individuals file suits saying the administration has gone too far with an investigation. That was the situation in *Watkins v. U.S*[83]. During the 1950s, Congress was keeping a keen eye on the communist movement in the United States. Communists were individuals from a political group that desired to overthrow the government. John T.

[82] (1990) 497 U.S. 261
[83] (1957) 354 U.S. 178

 ISSN: 2582-6433

Watkins, a labour union official, was called before Congress to affirm about known communists. Watkins however, refused to distinguish individuals who used to be, yet no longer were the members of the Communist party. Watkins was convicted for contempt of Congress for declining to respond to such inquiries, but the Supreme Court turned around his conviction. The Court said Congress does not have unlimited power to investigate the private lives of American natives.

Right to privacy cases came into the Information Age in *Whalen v. Roe*[84]. New York State had a computer system that had stored in it the names and addresses of patients who got doctors prescribed medicines. The system was intended to control the illicit utilization of such medications. Patients filed a lawsuit saying that the computer system abused their privacy rights[85]. The patients were under the fear that they would be called drug addicts if the public got access to the stored information. The U.S. Supreme Court held that the computer system did not damage the privacy rights as the fact that the law required New York to keep the prescription data secret. As computer become more dominant and store consistently huge amounts of data, Americans need to work more hard to ensure their right to privacy.

2.5 CONCLUSION

The researcher after analysing the various definitions of the scholars and authorized dictionaries and after exploring the concept and the different dimensions of the privacy in human life, draws the conclusion that Right to Privacy is an very essential right of the individual. It is so attached to the human existence as soul to the body and no citizen can enjoy his right to life with dignity which is provided to him by the law of land without the existence of the Right to Privacy. As studied in the chapter every aspect of the human life requires privacy as it may either be marriage, abortion, communication, information exchange or any other, but without the existence of privacy no person can stand up to these various phases.

CHAPTER: THREE

LEGAL FRAMEWORK RELATING TO PRIVACY AND AADHAAR

[84] (1977) 429 U.S. 589
[85] Lakhwinder Singh, *Right to Privacy & Freedom of Media* 56 (Eastern Book Publishing, New Delhi, 2016)

 ISSN: 2582-6433

ACT,2016

3.1 INTRODUCTION

In this chapter the researcher analyzes the different 'Legal Frameworks' which are presently operating in India and some which are pending in the parliament for the approval. In this chapter the researcher have discussed the constitutional provisions related to the 'Right to privacy' and several important provisions under different statues like Contract Act, Easement Act, Law of Evidence etc. The researcher have also undergone through the provisions of the Information Technology Act which are important as they guard the Privacy of an individual in the modern era of the Information and Data. The vital committees and latest schemes like Unique Identification Scheme, National Population Register in Indian Citizenship Act etc are also discussed. Human rights are those least possible rights people need against the state or other public authority by reason of their being part of the human family, regardless of some other consideration. The idea of human rights is established on the ancient doctrines of common rights dependent on the natural law. Ever since the start of edified life in a political society, the deficiencies and tyranny and ruling powers have driven individuals to look for higher laws. The idea of higher law binding human authorities was developed and came to be affirmed that there were sure rights prior to society. These were better than rights made by human authorities and were universally applicable before the advancement of the political social orders. The rights were simple belief and there was no agreed list of them and no such mechanism for their enforcement until they were arranged into national constitutions, as a judicially enforceable Bill of rights.[86]

The awareness of human rights has so grown that it is now used as a yard for measuring the civilisation of nations, sates, regimes and positive legislation. It is used both by people and by government as requirements for creating quality decisions.[87] It is used as Government and Authority limitations. It is used in every international financial and humanitarian aid as a means of growth.

As far the General Assembly of the United Nations obtained the Universal Declaration on Human Rights in 1948 and declared that "every individual is born free and equivalent in dignity and freedom in the world, and everyone is entitled for rights and liberties without prejudice of

[86] Chairanjivi J. Nirmal, *Human Rights in India: Historical, Social and Political Perspective* 1 (Oxford University Press, New Delhi, 2002)
[87] *Ibid.*

 ISSN: 2582-6433

any kind," the issue for human rights has taken on a worldwide dimension. Awareness to secure the human rights has developed to such a degree, that today it is being utilized as a measuring stick to quantify the progress of social orders, states, regimes and positive laws. It is being used a as criteria for making esteem decisions, both the people and Government. It is being used as limitations on the Governments and its authorities.[88] It is being utilized as vehicle of advancement in each International monetary and humanitarian aid Promotion and assurance of human rights guarantees predominance of freedom justice, harmony and order in every social order. It guarantees acknowledgment of worth of individual on equivalent basis. It guarantees that each individual possess a quality life based equality, dignity, regard and concern.

Cognizance of human rights is fundamental and important for each social order to live in harmony and fraternity. Recognition of human rights is a complicated one, more so in this multi-cultural, multi-lingual society like our own. However it is achievable through co-operations with every individual observing it in his relations with different people, groups and social orders. It is possible when every individual regards the life of different as his own and when every person think the respect of the others is as crucial as his own. For it's a human rights culture must be created in every part of the society.[89]

Human rights are general, sacred and inalienable in each individual. 'Privacy', as the most precious human right of all, is ensured in a few important national, regional and universal instruments. It has a few dimensions, including however not limited to privacy of an individual, individual communications, personal information and territorial privacy. The right to privacy which is the very fundamental aspect of one's life and individual freedom plays a huge role in the advancement of one's personality, integrity and pride. However, certain practices, for example, bugging, phone tapping and interception posing danger to the confidentiality of communications.

3.2 RIGHT TO PRIVACY IN INDIAN CONSTITUTION

The Constitution of India in general does not have any express provision regarding the Fundamental Right to Privacy but still by the means of judicial decisions the right is said to be under Part III of the Constitution. Following are the provisions which are said to have the provisions related to the ‘right to privacy’:

[88] *Supra note 85 at p. 34*
[89] Iyahit D.Naikar, *The Law Relating to Human Rights* 3 (Bangalore Fulani Press, Banglore, 2004)

 ISSN: 2582-6433

- *Article 19 : Freedom of Speech and Expression-*

  Part III of the Constitution of India is entitled 'Fundamental Rights' and lists several freedoms that are considered to be basic to all Indian people. Some fundamental rights, particularly the right to life and liberty, extend to all individuals in India, even if they are not 'citizens'. Article 19(1) (a) provides that "all citizens shall have the right to freedom of speech and expression." However, this is justified by Article 19(2), which says that it will not influence the implementation of any current law or stop the State from creating any law, insofar as such law imposes reasonable constraints on the practice of the right in the interests of India's sovereignty and integrity, state security, friendly ties with foreign countries, public order, decency or morality.[90] Article 13 prevents the State from creating any law which violates the Part III of the constitution.

  Consequently, the freedom of expression assured by Article 19(1)(a) is not an absolute right, but a competent right which, under the constitutional system, is capable of being curtailed under specific circumstances.

- *Article 21 : Right to Life and Personal Liberty-*

  Article 21 of India's constitution gives citizens and non-citizens the right to privacy[91]. This is not obviously stated in it, but as a statutory justification, the Supreme Court indicated the same. Article 21 of the Constitution states as follows: "No individual shall be denied of his lives or personal freedom except as provided by the procedure established by law."[92]

  Article 21 is the heart of Indian people's freedom. The terms "procedure created by law" in this article have been the subject of debate since the Indian constitution was enacted. The right strategy that is needed is that, in the sphere of personal freedom, the significance of the operation created by law is not very distinct from that of the due process clause of

[90] HM Seervai, *The Constitutional Law in India : A Critical Commentary* 43 (Central Book Publication, New Delhi, 2003)
[91] *Ibid.*
[92] JN Pandey, *Constitutional Law of India* 92 (Central Law Agency, New Delhi, 2007)

 ISSN: 2582-6433

the Fifth Amendment to the American Constitution.[93]

3.3 RIGHTS RELATED TO PRIVACY IN DATA PROTECTION LAWS

Information Technology Act, 2000 (herein after referred as IT Act, 2000) is the sole existing legislation in the country that keeps the privacy of an individual protected in the matters of Data and Information transactions. The Act has been amended in the year 2008 by the Indian legislature and added several provisions to the existing Act of 2000 to make them more effective in the field of protection. The Information technology Act and the Amendment Act 2008 have the following provisions that ensure the privacy in the Data related issues:

- *Section 30*- Section 30 of the Information Technology Act, 2000 needs the certifying authority to conform to safety processes to guarantee electronic signatures ' secrecy and privacy.

  Section 30 reads as, [94]

  Each Certifying Authority shall-

  a) Make use of interference and abuse-secure hardware, software and procedures

  b) Provide in its facilities a decent amount of reliability that is fairly suited to the results of the planned tasks;

  c) Adhere to safety processes to guarantee electronic signature's safety and privacy (inserted by Information Technology Amendment Act, 2008)

  a) Be the database of all certificates of electronic signature provided under this Act (inserted by Information Technology Amendment Act 2008).

  b) Publish data on its procedures, Electronic Signature Certificates and current status; and (inserted by Information Technology Amendment Act 2008)

[93] MP Jain, *The Constitutional Law of India*, 1175 (Lexis Nexis, New Delhi, 8th edn., 2018)
[94] The Information Technology Act 2000, s 30.

 ISSN: 2582-6433

d) Observe other standards that the laws may specify.

- *Section 43*- Section 43 of the Information Technology Act, 2000 provides sufficient provision for the person concerned to receive compensation for unlawful access to his private and personal data.[95] Under this section intrusion of one's computer or computer framework amounts to compensation. Several clauses and explanations of this section were amended by the ITAA 2008 which are clause (a), clause (i), clause (j), and explanation (v).

- *Section 43A (by Information Technology Amendment Act, 2008)* - This completely new section was added to the statute through the IT Amendment Act 2008. This section provides 'Compensation for inability to safeguard data- where an entity that possesses, distributes or handles any delicate private data or information in a computer resource that it possesses, monitors or works is negligent in applying and retaining appropriate safety practices and procedures and thus creates any individual unfair loss or unfair benefit, that entity is responsible to pay the losses by the way of compensation to the person who is affected.'[96]

- *Section 66*- Section 66 of the Information Technology Act, 2000 also protects sensitive private information residing in a computer resource as it makes, among others, a punishable decrease in the value of information residing within a computer resource with imprisonment for up to three years.[97] Thus, if an attacker is hacking into the computer system and copying and transferring sensitive personal information to a rival that may be of very high utility or of very private nature or business importance to the proprietor, the said act results in a decrease in the amount of data located within a computer resource and thus infringement of privacy.

- *Section 72* - Section 72 of the Information Technology Act, 2000 says about violation of confidentiality and privacy, i.e. a government officer can be fined if he transfers in his formal ability any digital information or data which he has obtained about an person.[98] There is only a limited implementation of this section. It is confined to the actions and omissions of those individuals who have been given authority under this Act, rules or laws

[95] *Id ;* Section 43
[96] *Id ;* Section 43A
[97] *Id;* Section 66
[98] *Id;* Section 72

 ISSN: 2582-6433

produced under it, i.e. police, certification authorities and officials approved by particular notice.

- *Section 72A*- this section was also added to the statute through the ITAA 2008. The section says; Punishment for disclosure of information in contravention of a lawful contract- Save as otherwise provided for in this Act or any other law in force for the time being, any person, including an mediator, who, while offering services under a legal contract, has obtained access to any material containing information about another person with the intention of causing or knowing that he is ought to cause the unlawful damage or unlawful profit reveals, without the approval of the individual involved or in violation of a legitimate agreement, such work shall be punished with probation for a period of up to three years or a penalty of up to five lakh rupees or both.[99]

3.4 THE DATA PROTECTION LAWS: INITIATIVE TAKEN BY LEGISLATURE

As by the emergence of new era of technological advancement the information and data became the new essential feature which demands the all over security of data from the intrusion by any third party or from the state itself. In this context the Indian parliament has taken the following initiatives so that the personal data of an individual can be secured and kept safe.

3.4.1 Parliamentary Standing Committee on Information and Technology

The committee presided by Anurag Thakur and the committee comprises of 31 members from the Lok Sabha and Rajya Sabha. Emphasizing on the need to tackle problems related to information security of public servers instantly, this Parliamentary Panel identified 14 approximately twenty topics from four ministries namely; Ministry of Information and Broadcasting, Ministry of Electronics and Information Technology, Ministry of Communications (Post Department) and Ministry of Communications (Telecommunications Department). This included concerns and difficulties including surveillance of social media to prevent the propaganda of terrorism; supervision of Web companies such as Facebook, Twitter, Google for Indian Consumers information security.[100]

[99] *Id;* Section 72A
[100] " Right To Privacy & Data Protection Laws In India" Economic Times, October 9, 2017

 ISSN: 2582-6433

The Committee will concentrate on providing a system for the state to assess "internet crime operations." It will also examine internet corporations collecting enormous amounts of information from Indian people in an effort to develop a scheme to safeguard their private information from leakage. One of the committee's focus will be internet data security.

3.4.2 Justice (Retd.) B.N Shrikrishna Committee

In accordance with the order of the Supreme Court in the case of Justice K.S. Puttaswamy, the Govt. of India has set up a committee of five members headed by former Supreme Court judge, Justice (Retd.) B.N. Srikrishna for drafting a Data Protection Bill. If the bill is passed, the Bill will be India's first inclusive legislation to safeguard the personal data of online users from abuses by state and non-state intruders.The Srikrishna Committee's office memorandum states that the govt is aware of India's increasing significance of data protection. It is of utmost significance to guarantee the development of the digital economy while maintaining individual's private information safe and secure.

The latest decision on privacy shows the position of the Committee in developing a solid information security system. The Court acknowledged the attempts of the government to implement the method of evaluating the complete data protection area. It notes that “leaving the matter for specialist determination would be suitable.”[101]

3.4.3 Factors Guiding the New Legislation on Data Protection

1) The Principles on Fair Information Practices-

In the 1980s, the principles were created as a reaction to enhanced automated information use, from the foundations of information privacy laws across most countries. The purpose of these principles is to guarantee that such collection is legitimate even when private information is obtained about an person and that the person includes the possibility of exercising power over it.[102]

The principles of fair information practice recommend the following minimum data privacy

[101] Krishnadas Rajagopal "For a robust data protection regime", The Hindu , September 8, 2017
[102] Akshita Gaur "Saving Privacy for Public Good ", Economic Times, September 15, 2017.

 ISSN: 2582-6433

requirements:[103]

a) Personal data shall be gathered with the individual's approval,

b) Its use shall be restricted to the collection task ;

c) Individuals must proceed to have access and rectification of their private information ;

d) The information must be precise ;

e) Organizations must also guarantee data security policies for the protection of private information.

Though India has no data protection statute, the rules on Information Technology Reasonable Security Practices and Sensitive Personal Data or Information was issued in 2011 under the I.T Act, aims to implement the principles of fair information practice in India. While the guidelines are a first effort to frame a legal data protection structure, they fall dramatically short of universally agreed norms of Data protection.

Firstly, they relate to a limited class of information considered in nature to be vulnerable. This involves data such as physical, physiological and mental health, gender determination, medical documents, biometrics, etc. Secondly, they only extend to the private sector, offering the state a free reign to obtain and use personal data from individuals as their choice.

It also enables for endless information sharing with the Indian government on wide basis such as prevention, monitoring, inquiry including cyber crimes, prosecution and penalty of offenses, etc., combined with a restricted duty on the govt not to reveal such information. Lastly, the lack of an autonomous a efficient implementation system implies that these laws are merely a toothless tiger.[104] In addition to IT regulations, scattered instruments across industries such as circulars published by the Reserve Bank of India requesting the implementation of privacy policies, the Credit Information Companies (Regulation) Act, 2005, and related rules, and terms of licensing contracts for telecommunications service suppliers, acknowledge restricted values of

[103] *Ibid.*
[104] *Supra note 101 at p.42*

 ISSN: 2582-6433

fair information practice. However, these too fall short in practice.

2) Experts report on Privacy, 2012[105]*-*

Headed by the retired chief justice of Delhi High Court A.P. Shah, it was formed by the national planning commission. Both the state and the Court decided that in the context of the fresh Data Protection Bill, this would be the "conceptual basis for laws safeguarding the privacy."

Before collecting their private information, the Justice Shah Committee had stressed on receiving the approval of the customers. It had suggested offering users previous notification of information procedures, making options available to them, and collecting only restricted data needed for the cause for which it is being gathered. If there is a cause modification, the person must be informed. Most crucially, the report suggested a data controller to provide customers with access to their private information. People should be prepared to pursue correction, modification or deletion of incorrect data.[106]

3) General Data Protection Regulations of European Union-

India requires a distinct data protection and privacy law, ideally in line with the aforementioned regulation enacted and scheduled to enter into effect in May 2018. In January 2012, the European Commission suggested an extensive revision of European Union information protection regulations aimed at giving people authority over their private information and simplifying the company regulatory framework.[107]

3.5 DRAFT LEGISLATION ON RIGHT TO PRIVACY

Since 2010, beginning with a view on privacy in India has been regarded as the outlines of a part of draft privacy laws published in 2011 and 2014. The 2014 edition was leaked and is still being proposed as of 2017, but if it became a statue it would acknowledge the right to privacy as a fundamental right under Article 21 of the Indian Constitution, set up a Data Protection Authority and set up an alternative dispute system to resolve conflicts between information controllers and people.India's govt set up an specialist panel to propose a Data Protection Bill in July 2017. Justice B N Srikrishna, Former Judge, Supreme Court, chairs the commission. The

[105] Rishika Taneja, Privacy laws In India , 33 (Eastern Book Company, Lucknow, 2014)
[106] *Ibid.*
[107] Anuj Sharma, " Data Protection Laws In India, Economic Times, September 15, 2017

 ISSN: 2582-6433

Expert Committee published a "white paper" in November 2017 for public discussion on the edges of India's privacy law. The Committee of Experts also conducted four open sessions in various Indian cities to obtain feedback on important elements of the suggested law.[108]

The Committee published its final study and draft data protection law in July 2018, called the Personal Data Protection Bill, 2018. The Personal Data Protection Bill offers for the creation of a Data Protection Authority to supervise information handling operations. It also acknowledges the need to safeguard private information in the context of the fundamental right to privacy, as well as the need to develop a mutual culture that promotes a safe and honest digital economy, respects citizen's information privacy and ensures freedom, advancement and creativity.

Furthermore, the Bill stipulates that it seeks to protect the independence of individuals with regard to their personal data, to define where the flow and use of personal data is suitable, to establish a relationship of assurance between individuals and institutions processing their private data, to determine the rights of persons whose private information are processed, and to establish a framework for the implementation of organisational and technical steps in the handling of private information, establishing standards for the transmission of private information across borders, ensuring the responsibility of information handling organizations and providing remedies for unauthorized and dangerous processing.

3.5.1 Key Provisions of the Draft Bill

The bill appears to obey the pattern of the General Data Protection Regulation of the European Union in its wide framework and on a variety of important clauses; the draft law holds powerful roles in the preservation of privacy. The draft bill included well-recognized values of privacy on how to send a notification to people before collecting information. It suggests that it must be safe, notified, particular, transparent and capable of being revoked in order for the approval to be legitimate, in addition to prescribe explicit permission for delicate private information. The draft bill also features objective restriction and collection restriction widely. Likewise, some of individual's main freedoms, such as the right to confirm and access, the right to rectification and the right to data portability, are component of the bill which would go a long way in giving people power over their information. Finally, it is extremely necessary to set up a data protection agency

[108] Pavan Duggal, *Data Protection Laws in India* 77 (Universal Law Publishing, New Delhi, 1st edn., 2016)

 ISSN: 2582-6433

and certainly it will contribute to a powerful, autonomous and dedicated agency[109].

- *Necessity in the bill-*

The "necessity" legal concept, established in international law and in numerous countries by constitutional and administrative courts, has been introduced into the drafting of India's data protection act. At this stage, it is worth investigating the meaning of limitations that the state may impose on privacy that have been mentioned in Puttaswamy's judgement. In the presence of provisions including Section 13 of the draft bill, it is necessary to check the privacy constraints in the manner of rejection of explicit consent against a statutory norm[110].

In the scenario of Puttaswamy, the bench was not needed to provide a legitimate test to evaluate the degree and complexity of the right to privacy, but they do provided us with adequate supervision to consider how to determine in future cases the boundaries and extent of the constitutional right to privacy. The three most effective tests conducted by Justice Chandrachud are-

a) The existence of "legislation"

b) A "lawful interest of the State"

c) The "proportionality" requirement

It is the ultimate 'proportionality' test described by the judgment of Puttaswamy that is most active in this sense. In contrast to sections 42 and 43 of the bill, which include 'requirement' and 'proportionality' as twin tests, the commission chose to use only one ground in Chapter III.

In many cases, the use of "necessity" in the proposal mirrors how the term is used in the European Union's General Data Protection Regulation. Use of 'necessity' in section 13, for example, is obviously derived from the General Data Protection Regulation's language. But, unlike countries like the, Canada, and South Africa and European Union that have a wealthy background of legislation over the word, India has no legal guide on how to understand it. If the Srikrishna commission planned to embrace the concept of 'necessity' as expressed by the

[109] Available at : http://www.mondaq.com/india/x/801302/Data+Protection+Privacy (Visited on 28 June, 2019)
[110] *Ibid.*

 ISSN: 2582-6433

'European Commission'. The definition that followed the proposal should have been obviously stated in its study. This would have presented the data protection agency and the judiciary with explicit instructions about how 'necessity' should be interpreted. It is also significant that as regards non-state actors, the bill relates to 'necessity' as a norm.

'Necessity' has developed in the jurisprudence of constitutional law to regulate interference with citizen's fundamental freedoms. The way it is constructed in India is therefore strongly dependent on knowing the extent and restrictions to fundamental rights and how they could be curtailed. At this point, the circumstances for non-consensual processing depend only on requirement, and not on proportionality[111].

- *Data Localisation-*

A copy of all private information gathered on a computer or data centre situated in India will be needed by all information distributors as per the draft bill. This was implemented to address information request issues experienced by research organizations when they request information hosting outside India. Localization mandate is unlikely to solve this problem for two purposes. First, as acknowledged by the Committee itself, regarding the information being physically deposited in India, a breach of law issue may still occur. Second, the mandate for localization only applies to Indian people. This does not resolve the issue that emerged in a situation where law enforcement agencies require access to foreign information. India would be quite better if it were to best express its role in diplomatic talks using the language of international law.

- *Regulations Regarding Surveillance-*

The draft Bill involves paired tests of "necessity" and "proportionality" as a basis for any processing for government security reasons; and avoidance, surveillance, inquiry, and prosecution of law infringements. However, there is no duty and transparent procedure for the organizations concerned to create 'necessity' and 'proportionality' before a legislative or quasi-judicial body in its present implementation. Certain clauses, such as notification of users, limitation of retention periods and a restricted right to verification, access and redress, are presently totally absent from the Bill.

[111] R. Dhiruswami, "Privacy & Data Protection laws" 6 JLCW 34 (2017)

 ISSN: 2582-6433

3.5.2 Proposed Legislation on DNA Profiling

Since 2007, a DNA profiling proposal has been debated in India. The latest draft proposal, "Use and Regulation of DNA Based Technology Bill 2017," is the most current repetition of laws following the past draft bill's in 2012 and 2015.[112]If adopted, the 2017 proposal would set up domestic and regional DNA databases with five distinct indicators:

An overview of the crime scene, missing individuals, offenders, suspects and unidentified dead individuals. Data from the DNA databases will be accessible in six conditions: to law enforcement and investigating authorities, in court trials, to facilitate prosecution and arbitration of criminal instances, to take defence of an accused, to investigate civil conflicts, and other instances that may be stipulated by legislation. There are crimes involving unauthorized access or use of DNA bank data, including unauthorized disclosure, and acquiring data without authorization.

3.6 IDENTIFICATION SCHEMES UNDER RIGHT TO PRIVACY

There are two national identification databases in India: the Unique Identification database also referred as Aadhaar, and the National Population Registrar. Other materials, in relation to these two databases, are used as evidence of identity such as passports, PAN cards, ration cards, driving licenses, and election records.

3.6.1 Adhaar- The Unique Identity Scheme

The Unique Identity Database system is the biggest digit system in the world. The Unique Identity Database system was first introduced in 2010, and in April 2016, Aadhaar registration achieved 1 billion registrations. The system aims to issue a 12-digit identification number to each citizen of India depending on his / her biometric information that contains; fingerprints, retinal scans, and photos; and also voluntarily contains demographic information such as email, name, family name, and age. The figure is called the Aadhaar number. People must visit registrars and registration centres with the suitable paperwork to register in the Unique Identity Database.Registration centers are institutions that are working with India's Unique Identity Database Authority and registrars can be both public and private. Once documents have been inspected and biometrics are collected, an confirmation note will be sent to persons and their

[112] Ian Llyod, *Information technology law* 78 (Oxford University Press, New Delhi, 2017)

 ISSN: 2582-6433

Unique Identity Database code will be sent in the email. India's Unique Identity Database Authority would own and run a Central Identity Data Repository, a centralized project that contains each citizen's biometric and demographic information. The number can be utilized during transactions and when retrieving government facilities to verify the identity of people.[113] To allow service delivery, the Aadhaar number of an person is put into the service operator's database. Under the Department of Electronics and Information Technology, biometric technology used in the system must be approved by the Directorate of Standardization Testing and Quality Certification. Certified providers are: Bio-Enable Technologies, Inspirited IT Solutions and Services, Precision Informatics, Madras as of November 2015[114].

The Unique Identity Database system is managed by India's Unique Identification Authority, an institution established by the Government of India as an associated department of India's Planning Commission by the notification no. A.03011/02/2009-Ad. Justice K.S. Puttaswamy submitted a written petition to the Supreme Court of India in 2012 criticizing the state's strategy of creating an Aadhaar card compulsory for each individual in India and its successive plans to connect different government reward schemes to the card. On 23 September 2013, the court issued an provisional order stating that no individual should be discriminated in accessing facilities because they did not have an Aadhaar card. On 11 March 2016, the Lok Sabha enacted the Aadhaar Targeted Delivery of Financial and Other Subsidies, Benefits and Services Act, 2016 to set up a legislative structure for the Aadhaar system.[115]While for a variety of purposes the Aadhaar Act has been argued and criticized, it also has a number of consequences for privacy, some of which are discussed below in short:

(i) The Aadhaar Act, by submission of its biometric data and demographic data under Section 3(1) of the Aadhaar Act, enables every "resident" to acquire an Aadhaar amount. It has been stipulated that race, religion, caste, tribe, ethnicity, language, entitlement documents, earnings or medical history will not include demographic data. Thus, even though the Act explicitly gives what data can be gathered, the acquisition of additional data is not expressly forbidden. A resident is described as every individual residing in India prior 12 months for a minimum period 182 days.

[113] Jyoti Rattan, *Cyber laws & Information Technology* 67 (Bharat Law House, New Delhi, 2017)
[114] *Ibid.*
[115] J. Yatindra Singh, *Cyber Laws* 87 (Universal Law Publishing, New Delhi, 2016)

 ISSN: 2582-6433

(ii) Under the proviso of Section 28, the Aadhaar Act offers that owners of Aadhaar numbers may seek access to their identification data from India's Unique Identity Database Authority other than their key biometric data. It is not apparent why an person is not supplied with access to the key biometric data that is described as fingerprints, eye scans or other genetic characteristics that laws may specify. Furthermore, section 6 appears to be responsible for upgrading and guaranteeing the reliability of the person's biometric information. It is not evident how a individual should know that the biometric data stored in the database has altered that he or she has no access to this information[116].

(iii) The Aadhaar Act provides people the opportunity to demand that their demographic data be altered by India's Unique Identity Database Authority if the same is inaccurate or has altered and biometric data if destroyed or altered under Section 31. This section offers for the modification of identity data, but only under the situations specified in the section, e.g. demographic data cannot be amended if it has been destroyed or lost, similarly biometric information cannot be altered if it is incorrect.

(iv) While under Section 8(4), India's Unique Identity Database Authority is permitted to respond to any verification request with a favourable, negative or other suitable reaction and it may exchange identification data with the proposing organization, with the exception of key biometric data.

(v) India's Unique Identity Database Authority has been provided the capacity to designate one or more organizations under Section 10 to create and retain the Central Identity Data Repository also called CIDR.

(vi) Biometric data collected by India's Unique Identity Database Authority has been considered to be an "electronic record" as well as "sensitive personal information" under Section 30 of the Act, meaning that, in relation to the regulations of the Adhaar Act, the provisions of the Information Technology Act, 2000 will also extend to such data. It should be observed that while the Aadhar Act describes the concept that India's Unique Identity Database Authority is needed to guarantee data security, it does not develop rules on the lowest possible security norms that the Authority must enforce. The government has, however, related the safety requirements specified in the Information Technology Act with the biometric data discussed in the Aadhaar Act through this section.

3.6.2 National Population Register

[116] *Supra note 112 at p. 47*

 ISSN: 2582-6433

The National Population Register is lawfully based on the regulations of the 1955 Citizenship Act and 2003 Citizenship Rules. Under National Population Register, registration in the National Population Register in accordance with Section 14A of the Citizenship Act, 1955 is compulsory to every citizen of India. Data collection started in 2010 with the National Population Register system. The Electronics and Information Technology Department manages the information gathered within this system.[117]

The repository of the National Population Register will include thirteen demographic data classes and three biometrics classes. The Citizenship Rules do not enable the compilation of biometric data and are supplied through instructions. This is in accordance to the National Population Register of the Department of Information Technology. The practices to be pursued for developing the National Population Register was set out in the Citizens Registration and National Identity Card Rules of 2003, and the recommendations are released from time to time. The gathered biometric data includes two retina scans, ten fingerprints, and a photograph. Only the photographs and fingerprints were originally designed to be collected, as per a 2010 Committee note, whereas the retina scans were introduced later. Biometrics replication is presently relocated to India's Unique Identification Authority and personal companies are delegated to collect biometrics.

A dual collection method is involved in the National Population Register. A door-to-door collection of data is performed as part of the Survey in the first stage, by means of a questionnaire without authentication or supporting documentation. A checking method is accompanied by a government demonstration of the data. This information is digitized afterwards. Then the information participants will offer their biometric information on the manufacturing of the survey tip in the information gathering centres. Biometric information gatherers are entities that are picked out by India's Unique Identity Database Authority and are qualified under the Unique Identification Database System to gather information. The information of a person is consolidated and then replicated by India's Unique Authority for Identity Database[118].

The National Population Register Identity Data Card is suggested to be a microprocessor chip smart card and every person's demographic and biometric characteristics will be customized in this card together with the Unique Identity Data number. The state is currently only discussing

[117] Vakul Sharma, *Information Technology Law & Practice* 83 (Lexis Nexis, New Delhi, 5th edn., 2016)
[118] Vijay Rattan, *Cyber laws & Information Technology* 56 (Asian Book Publishing, New Delhi, 2017)

 ISSN: 2582-6433

the option of smart cards being distributed to all citizens over the age of eighteen.

3.7 REGIONAL POLICIES & INITIATIVES

The two main areas in which the government of India has took the liberty to look at and take initiatives so as to frame policies for the security against them. These are:

- *Cyber Security-*

A National Cyber Security Policy was released by the state in 2013. The Policy created a mechanism for ensuring Indian cyberspace and sets out the want, to construct a domestic authority to monitor cyber safety projects, develops a system for certainty, promote the use of open source software products and facilities, generate a vibrant legislative framework for cyber security, and secure defence warning systems, safe e-government facilities, improve cyber security.

The Standing Committee on Information Technology, 2013-2014 study observed that a range of legislative measures had not yet been enacted and suggested the creation of a National Critical Information Protection Centre and a centralized agency to tackle cyber crime in India. The Committee also observed the need to create ability and a legal structure in India to safeguard privacy[119].

- *Cyber Crime-*

In the IT Act, cyber crime is dealt with lawfully, such as the following sections:

1) Section 43: Causing computer harm, computer system damage etc.

2) Section 43(a): Access or secure access to these computers, computer systems or computer networks or computer resources.

3) Section 43(b): Download, copy or extract any data, computer database or data from computer, computer system or computer network, including information stored or positioned in any removable storage device.

[119] Anirudh Rastogi, *Cyber Law: Law of Information Technology* 90 (Lexis Nexis, New Delhi, 2014)

 ISSN: 2582-6433

4) Section 43(c): Produce or cause any computer contaminant or computer virus to be implemented into any computer, computer device or computer network.
5) Section 43(d): Harming or causing damage to any computer, computer device or computer network, information, computer database or other programs in that computer, computer system or computer network[120].
6) Section 43(e): Disrupt or disrupting any computer, computer system or computer network.
7) Section 43 (f): Denial or rejection of access by any means to any individual permitted to access any computer, computer system or computer network.
8) Section 43 (g): To assist any individual in facilitating access to a computer, computer device or computer network in violation of the requirements of this Act, the regulations or laws laid down therein
9) Section 43 (h): Charging a person's facilities to another person's account by controlling or tampering with any computer, computer system, or computer network.
10) Section 43 (i): Destroying, erasing or changing any data that resides in a computer resource or, by any means, decreasing its importance or utility or injuriously influencing it.[121]
11) Section 43 (j): Steal, hide, destroy or change or lead any individual to steal, hide, destroy or change any computer source code which is used for a computer resource intended to cause harm.
12) Section 44: Failure to provide data, etc ;
13) Section 67A: Publishing or communicating in electronic form content that contains sexually specific behaviour, etc. ;
14) Section 66D: Cheating using any communication tool or computer resource by impersonation ;
15) Section 66F: Cyber terrorism indulgence as described in the Act ;
16) Section 67B: Publication or transmission in electronic type of content portraying children in a pornographic act, etc. ;
17) Section 43A: Data protection failure ;
18) Section 66E: Capturing, posting or communicating purposely or willingly the picture of any person's private region without his or her permission, in conditions that violate that individual's privacy ;
19) Section 45: Failure to comply with the laws, rules and regulations.

[120] *Ibid.*
[121] Farooq Ahmed, *Cyber Laws in India* 46 (Allahabad Law Agency, Allahabad, 2017)

 ISSN: 2582-6433

20) Section 66B: Receiving or maintaining dishonestly any robbed computer resource or communication equipment that knows or has cause to consider the same thing to be robbed.
21) Section 67: Electronically publishing or communicating pornographic content;
22) Section 66C: Use of any other person's digital signature, password or other distinctive identifying function fraudulently or dishonestly ;

In addition to the above offenses, there is also a clause in the Information Technology Act that provides legal recognition to electronic records. Thus, if committed by electronic means, any offense that can be committed through physical document would also be regarded an offense.

3.8 RIGHT TO PRIVACY IN OTHER STATUTES

As known to all privacy is not a new concept. Although it is not an exclusive right but it has its traces all over in different statutes in different provisions. Some of the statutes which have the provisions relating to privacy are as follows:

3.8.1 Hindu Marriage Act, 1955

Section 22 of the Hindu Marriage Act, 1955 offers that no individual shall be permitted to print or post any information relating to the proceedings in camera without receiving the court's previous approval. The court's authority to withhold or approve the publishing of the trials in camera shall be regulated by factors of' public policy' or for purposes linked with' public order' or' state security,' etc., if any individual prints or releases any matter contrary to the provisions of subsection (1) it shall be punishable with a penalty of up to one thousand rupees.[122]

3.8.2 Indian Easement Act, 1882

Pursuant to Section 18 of the Indian Easement Act, 1882 offers that an easement may be obtained on the basis of a local practice which is called usual easement. Illustration (b) of the above section establishes the elements of the usual privacy right more or less. It lies down that no proprietor or occupant of a building can open a window, as by the custom of a town, in such a way as to significantly violate the privacy of his neighbour. A create a town house close the home of B. A, there on acquires an easement that B does not open a window in his house to order

[122] Hindu Marriage Act, 1955, s.32

 ISSN: 2582-6433

a view of the parts of A's house which are usually removed from consideration, and B acquires a similar easement as regards A's house.[123]

The scope of this usual right is primarily focused around concerns about the house of a newly created building or the modification of the original ones, the creation of a gate or window or the extension of the current ones, the design of a floor or balcony and the opening of a new entrance or the extension of the existing ones by the defendant; where, in particular, the plaintiffs home that part of the house that is usually isolated from inference and/or occupied by the female of his / her family is revealed to the defendant's view amounting to an intrusion of the privacy of the plaintiff.[124]

3.8.3 Indian Penal Code, 1860

"Privacy invasion", as an offense in the Indian Penal Code, 1860 was not brought from England; in fact it is the codification of the long-established traditions of the Indian people. Indian Penal Code, 1860 under section 228 A, gives for any individual who prints or publishes the title or any matter that discloses the identity of any individual against whom an offense under Section 376, 376A, 376B, 376C or 376D are claimed to be committed or found to be committed shall be punished with the prison term of either for a period of two years and shall be subject for fines.

Furthermore, section 509 of the code provides that any person who intends to offend the modesty of any woman speaks any word, makes any noise or expressions or displays any item, intends that such word or sound be heard or that such expression or item be seen by such a woman or encroaches into the privacy of such a woman shall be rewarded with simple jail for a term of one year or with fine or both.[125] Intimacy is the most private choice of an individual. One's right to choose either to have intercourse or not, with whom to have it and with whom not, etc; are an individual's personal choices and form the eminent part of his privacy. So the Indian Penal Code has several provisions regulating the offences related to intimacy as:

Under section 493 of the Indian Penal Code[126], anyone who, by misleading means, leads any woman, not legally married to him, to think that she is legally married to him and is responsible to punishment for cohabitation or sexual intercourse with her.Section 497, Indian

[123] Indian Easement Act, 1882, s.18
[124] *Supra note 120 at p. 53*
[125] Indian Penal Code, 1860, s.509
[126] Id; Section 493

 ISSN: 2582-6433

Penal Code punishes the offense of adultery pursuant to Section 498, Indian Penal Code; any person who takes or incites any married woman to commit unlawful sexual intercourse is also responsible for punishment.[127]

Religion, under the Indian Constitution is left to an individual's personal choice which makes it one's private affair. Section 295 to 298 of the Indian Penal Code, 1860 protects the individual's religious privacy as offences under these sections are punishable with both imprisonment and fine.

Another ambit of one's personal and private life is one's sexual orientation. Homosexuality prior to the year 2018 was an offence under section 377 of the Indian Penal Code, 1860 but after the case of *Navtej Singh Johar v. Union of India*[128] it was declared legal upto the extent of bestiality.Many offences like theft, robbery, extortion, criminal trespass, house breaking etc are some examples of the acts which are of such nature that they intrude the privacy of an individual but Indian Penal Code, 1860 provides both the penalty and punishment if such mentioned offence breaching the privacy right of the individual is committed.

3.8.4 Children Act, 1960

Section 36 of the Children Act, 1960 declares it unlawful if anyone makes any dispatch to any newspaper or magazine that discloses the name, address or school or any other information that may subject to the detection of the child involved in any litigation under the Act, including the publication of his photo.[129]

3.8.5 Copyright Act, 1957

Copyright, under the Copyright Act 1957, is a right given to authors of literacy, theatre, music, compute, and art works and cinema and audio recording manufacturers. Copyright covers the right to reproduce, communicate to the public, interpret and translate the work. Section 57 of the Act says that, if the work is harmful to his honour or reputation of the author, he is entitled to assert his credential and hold or claim damage in regard of any distortion, mutilation, alteration or other act in regards to the work. Even after the economic rights are given, moral rights are

[127] Id; Section 497
[128] WP (Cr.) No. 76/2016
[129] Children Act, 1960, s.36

 ISSN: 2582-6433

also made accessible to the authors.

3.8.6 Credit Information Companies (Regulation) Act, 2005

Credit Information Companies (Regulation) Act 2005 deals with the crucial parts of credit information reliability and safety by enabling the distribution of data to customers of credit information corporations and, at the same moment, providing for the preservation of the consumer's privacy. Credit information supplied by the credit information corporation shall be correct, comprehensive, properly handled and secured from failure or unlawful access or use, at the responsibility of the credit information corporation.[130]

Section 20 of the Act lists the values of privacy that apply to the credit information business, credit institution and the user indicated. The concept has been applied to process, record, preserve and secure information or data. The customer's or borrower's privacy shall apply to information uses, extent of the credit information company's responsibility, protection of credit information networking of credit information companies credit institutions, and any other principles and procedures.[131]

3.8.7 Indian Post Office Act, 1898

Indian Post Office Act 1898, Under Section 2(i) offers that, any entity authorized to take and distribute the postal item, including a passport, postcard, daily journal, book model, package and all transmissible by post, shall be responsible for penalty if discovered guilty of negligence endangering the security of postal items, triggering delay in the shipment or distribution of same. If any post officer pursuant to his responsibility, opens any postal item during postal transport, or willingly detains or delays such postal items, he is responsible for penalty. It is punishable for the detention of mails or any postal items or even for the opening of the mail bag by any individual without prior power under the Indian Post Office Act or any other Act in force at the moment.[132]

3.8.8 Right to Information Act, 2005

In a democratic system, the state has a duty to reveal the data produced for the benefit of the individuals at its level. There is no question that all the data that the state government

[130] Kshitij Dua, "Prevention is better than Cure", 23 IJL 8 (2006)
[131] *Ibid.*
[132] Indian Post Office Act, 1898, s.63

 ISSN: 2582-6433

department maintains in records is for the individuals, and that allows the individuals to have an assumed right to access that data. One of the main ideals of administration is that the officials dealing with individuals should be transparent and that data should be made available to individuals. Since the officials tend to believe themselves to be the bosses of individuals, remembering that they are assigned to represent the people's interests, it is necessary to specify that individuals have the right to information that the officials hold in their limits. As a result of democratic battles and disturbances over centuries and decades, this took the form of a legislative right. In the year 2005 the President of India gave its assent to the Right to Information Act and brought it to life.[133]

Right to Information Act, 2005 allows people to obtain data under the command of the govt. The privacy of patients and researchers, particularly those in public institutions, could be believed to be threatened. The purpose of this Act was to encourage public accountability in the state so that the privacy of persons who use public clinics or engage selflessly in government-funded studies could not be violated. Broadly speaking, the Act does not damage the secrecy of the partnership between the doctor and patient or the subject or researcher.[134]

Section 8(1) of the Act deals with "what's not available to transparency," the Act states that the information relevant to personal data access which is not related to any government action or interest, or which would trigger an unjustified breach of persons privacy should not be revealed. Moreover, the same section specifies that "Information accessible to a individual in his or her fiduciary relation such as a doctor's or academic's with a patient or student must not be revealed; until and unless a qualified authority is convinced that, perhaps the greater public interest is justified by such revelation of information.

3.8.9 Indian Evidence Act, 1872

Section 126 of the Indian Evidence Act, without the express approval of his client, a lawyer is not allowed to reveal any information produced to him during the practice of his job and for the benefit as a lawyer. Also, he shall not reveal the information or situation of any document he has become associated with in the span of his professional work or any guidance provided.

The duty thus placed on him remains even after his job has expired. The interpreters and

[133] Sudhir Nair, *The Right to Information in India* 45 (Oxford University Press, New Delhi, 2013)
[134] Right to Information Act, 2005, s.5

 ISSN: 2582-6433

such assistants of the Lawyer are also under the same responsibility. Furthermore, no one shall be forced to reveal any classified communication between himself and his counsellor to the court.[135]

Disclosure of any communication between the husband and wife by any person is also prohibited under section 122 of the Indian Evidence Act.

3.8.10 Indian Contract Act, 1872

Indian Contract Act deals with other means by which parties may decide to control the collection and use of private information collected, such as through a "Privacy Clause" or a "Confidentiality Clause". Parties to a agreement may therefore consent to use the disclosure of private data of an individual, with the appropriate consent and authorization of the person in a decided way and for accepted purposes; and any inappropriate submission of information which contrary to the explicit terms of a contract, would constitute a violation of the contract under the Indian Contract Act and would call upon for the damages as a result of any failure to comply with the conditions of the contract pursuant to section 74 of the Indian Contract Act, 1872.[136]

The company may request private data from an individual in an insurance agreement relevant to his family, background, racial origin, ethnicity, childhood, schooling, medical records, immediate family data, age, occupation, etc. In the situation of information processing businesses, there may be doubts about the qualified pursuits of an individual's earnings, investment choices, preferences, habits of expenditure, etc. Any violation of such a contract would enable the insurer's client to bring an action for breach of contractual conditions.

3.9 CONCLUSION

The researcher in this chapter has analysed the several existing legal frameworks which are related to the Right to Privacy and Data Protection in India. The legal framework includes firstly the Constitutional provisions i.e. Article 19 and the Article 21 of the Indian Constitution. The provisions of the Information Technology Act, 2000 and Information Technology Amendment Act 2008 are also discussed in this chapter as these very provisions provide support to the Data

[135] Indian Evidence Act, 1872 (Act no. 1, 1872)
[136] Abhinav Mishra, *Indian Contract Act 1872* 89 (Upkar Prakashan, New Delhi, 2014)

 ISSN: 2582-6433

or Informational Privacy to the individual by criminalizing or penalizing the breach of data in this modern era of technological advancement. The committees such as 'Parliamentary standing committee on IT' and 'Justice B.N Srikrishna committee' are also focused in this chapter. The draft legislation like 'Personal Data Protection Bill, 2018' and it's key provisions are also analysed. The role of popular identification schemes such as 'Aadhar' and 'National Population Register' is also accessed in terms of privacy and data protection in India. The researcher has in the end has analyzed many other legislations like Indian Evidence Act, Indian Penal Code, etc which have the provisions relating to the protection of privacy of the individual.

CHAPTER -FOUR

JUDICIAL APPROACH WITH SPECIAL FOCUS ON KS PUTTASWAMY VS UOI JUDGEMENT

4.1 INTRODUCTION

"Protection" and "justice" goes are the two facets of the same coin. Laws and liberties are the main 'principles' which have been influencing the establishment of 'the concept of justice and protection' in the society' since the old times. These two terms are so closely related to each other that they can be said to be complementary and supplementary for one another. The Judiciary is the main functioning body which has always worked in such direction to establish protection; weather of one's social or the personal life from the unwanted intrusions. Judiciary is one of the most important pillar of the democracy. It ensures the justice in the society. Judiciary through its interpretations have raised the concern for the right to privacy and data protection in society. Supreme Court as the guardian of the constitution has the power to interfere in any state organ to ensure the protection of individuals fundamental freedoms. As privacy and its protection in every form makes itself the part of Article 21 of the constitution. In this chapter researcher will discuss the several judicial approaches which Supreme Court has used to propound through its decisions. Underneath is the hierarchy of such important decisions which has setup the permanent structure of right to privacy and data protection framework:

4.2 EXPANSION OF ARTICLE 21 IN RESPECT OF RIGHT TO PRIVACY AND K.S. PUTTASWAMY VS. UNION OF INDIA JUDGEMENT REAFFIRMED THE RIGHT

 ISSN: 2582-6433

TO PRIVACY AS A FUNDAMENTAL RIGHT

A.K Gopalan v. State of Madras[137], in this case It is defined as freedom in relation to or in relation to the individual's person or property ; and in this context, personal freedom is an antithesis of physical restraint or coercion.

The phrase is broad enough to acquire the right to be free of constraints imposed on his activities. In the modern age, the term "coercion" cannot be interpreted in a limited context. In an uncivilized culture where there are no inhibitions, only physical restrictions can detract from personal freedom, but psychological restrictions are more effective than physical restrictions as civilization progresses. The science techniques used to shape a man's mind are, in a true context, the physical constraints, because they give rise to physical dread by channelling one's behaviour through expected grooves. So it could also be defined as physical restraints to create circumstances that inherently generate inhibitions and clusters of dread. In addition, the right to personal freedom encompasses not only the right to be safe from constraints imposed on his activities, but also the right to be safe from infringements on his private lives. It is accurate that our Constitution does not explicitly state a right to privacy as a fundamental right, but that right is a basic component of personal freedom.

Every democratic nation sanctifies national lives; remainder, physical joy, peace of mind, and safety are supposed to be given to it. In the last resort, his "fort" is the home of an individual, where he resides with his relatives; it is his rampart against his personal liberty being infringed. If physical restraints on the activities of a person impact his personal freedom, it would be affected to a greater degree by physical encroachments on his private lives. In fact, nothing harms the physical happiness and health of a man more than a calculated interference with his privacy. Therefore, in Article 21, we would describe the right of personal freedom as an individual's right to be safe from limitations or infringements on his person, whether those constraints or infringements are enforced immediately or indirectly by calculated interventions. It was thus recognized that all monitoring acts pursuant to Regulation 236 infringe the petitioner's basic right under Article 21 of the Constitution[138]."

R.C Cooper v. Union of India[139], in this case procedure laid down by law has acquired substantive due process component in Article 21, and even the contents of the law may be

[137] AIR 1973 SC 1461
[138] *Supra note 159 at p. 74*
[139] 1970 1 SCC 248

 ISSN: 2582-6433

questioned because they do not comply with the demands of the law. Consequently, given that the right to privacy is acknowledged as a fundamental right, current territorial legislation may now have to cross the rigors of the aforementioned exam if it is called into question. If privacy stayed merely a statutory or common law right, the same would not have been the stance.

Maneka Gandhi v. Union of India[140], the Apex court stated that right to privacy is secured as a basic part or essential feature which is guaranteed by part III of the Indian constitution which have initiate the position that privacy is a part of right to life which is essential for a human being to survive in the society under Article 21 of the constitution as a part of the freedom. This case highlights the expansion of the personal liberty as a fundamental right of the Indian constitution. In this case judiciary interpreted the privacy in the literal sense and not in a restricted way.

A.D.M Jabalpur v. Shivkant Shukla[141], in this case the chief justice of India explained the importance of privacy as a fundamental right. The privacy is a concomitant of right of the person to control over his personality.

Justice K.S.Puttaswamy(Retd) vs Union Of India[142] This case is the cornerstone of the 'Right to Privacy' jurisprudence in India. The nine Judge Bench in this case unanimously reaffirmed the right to privacy as a fundamental right under the Constitution of India. The Court held that the right to privacy was integral to freedoms guaranteed across fundamental rights, and was an intrinsic aspect of dignity, autonomy and liberty.

The case began with the question of whether the right to privacy was a fundamental right, which was raised in 2015 in the arguments concerning the legal validity of the Aadhaar database. The Attorney General appearing for the State argued that the existence of the right to privacy as a fundamental right was in doubt in view of the two decisions in the cases of M.P. Sharma vs. Satish Chandra[143], District Magistrate, Delhi , rendered by an eight Judge Bench, and Kharak Singh vs. State of Uttar Pradesh[144] , rendered by a six Judge Bench. Both the cases, the State argued, contained observations that the Constitution did not specifically protect the right to privacy as a fundamental right. At the same time, several subsequent judgments over the years

[140] AIR 1978 SC 579
[141] AIR 1976 SC1207
[142] AIR 2017 SC 4161
[143] 1954 AIR 300
[144] 1963 AIR 1295

 ISSN: 2582-6433

had recognised the right to privacy as a fundamental right. However, these subsequent decisions that affirmed the existence of the right to privacy were rendered by benches of a smaller strength than M.P. Sharma and Kharak Singh. Due to issues relating to the precedential value of judgments and noting the far-reaching importance of the right to privacy, this case was referred to a nine Judge Bench of the Supreme Court.

The Bench unanimously held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution". In doing so, it overruled previous judgments of the Supreme Court in M.P. Sharma and Kharak Singh, insofar as the latter held that the right to privacy was not recognised under the Indian Constitution.

In addition to cementing the place of the right to privacy as a fundamental right, this case also laid down the need for the implementation of a new law relating to data privacy, expanded the scope of privacy in personal spaces, and discussed privacy as an intrinsic value

Issue

Whether the right to privacy was a fundamental right under Part III of the Constitution of India

Arguments

The Respondents mainly relied upon the judgments in the cases of M.P. Sharma, as well as the case of Kharak Singh, which had observed that the Constitution did not specifically protect the right to privacy. The judgments were pronounced by an eight Judge and a six Judge Bench respectively, and the Respondents argued that they would therefore be binding over the judgments of smaller benches given subsequently. The Respondents further argued that the makers of the Constitution did not intend to make the right to privacy a fundamental right.

On the other hand, the submission of the Petitioners was that M.P. Sharma and Kharak Singh were founded on principles expounded in A.K. Gopalan vs. State of Madras[145]. The Petitioners argued that A.K. Gopalan, which construed each provision contained in the Chapter on fundamental rights as embodying a distinct protection, was held not to be good law by an eleven Judge Bench in Rustom Cavasji Cooper vs.Union of India[146]. Hence, the Petitioners submitted that the basis of the two earlier decisions was not valid. It was also urged that in the seven Judge

[145] AIR 1973 SC 1461
[146] 1970 AIR 564

 ISSN: 2582-6433

Bench decision in Maneka Gandhi vs. Union of India[147] , the minority judgment of Justice Subba Rao in Kharak Singh was specifically approved while the decision of the majority was overruled. In addition to this, other arguments made during the hearing dealt with the scope of the right to privacy. The Petitioners argued for a multi-dimensional model of privacy as a fundamental right, while the Respondents stated that the right to privacy was an ambiguous concept and could only be crystallized as a statutory and common law right.

The Petitioners argued that the Constitution would have to be read in line with the Preamble, while keeping in mind that privacy was a natural right, and an international human right. The Respondents advocated for a narrow approach which focused on the Constitution as the repository of fundamental rights and the Parliament as the only body which had the powers to modify the same.

Decision

The Supreme Court, through six separate opinions, pronounced privacy to be a distinct and independent fundamental right under Article 21 of the Constitution. The crux of the decision spelled out an expansive interpretation of the right to privacy - it was not a narrow right against physical invasion, or a derivative right under Article 21, but one that covered the body and mind, including decisions, choices, information and freedom. Privacy was held to be an overarching right of Part III of the Constitution which was enforceable and multifaceted. Details regarding the scope of the right were discussed in the multiple opinions.

he Court overruled the judgments in M.P. Sharma, and Kharak Singh[148], insofar as the latter held that the right to privacy was not a fundamental right. With respect to M.P. Sharma, the Court held that the judgment was valid for maintaining that the Indian Constitution did not contain any limit to the laws on search and seizure analogous to the Fourth Amendment in the United States Constitution. However, the Court held that the Fourth Amendment was not an exhaustive concept of privacy and an absence of a comparable protection in the Constitution did not imply that there was no inherent right to privacy in India at all – and therefore the conclusion in M.P. Sharma was overruled. The Court rejected the insular view of personal liberty ("ordered liberty") adopted by Kharak Singh, which Justice D.Y. Chandrachud referred to as the "silos" approach borrowed from A.K. Gopalan[149]. The Court observed that this approach of viewing fundamental rights in water-tight compartments was abrogated after Maneka Gandhi. The Court further observed that

[147] 1978 AIR 597

[148] *Supra note p.86*

[149] *Supra note p.86*

 ISSN: 2582-6433

he majority opinion in Kharak Singh suffered from an internal contradiction, as there was no legal basis to have struck down domiciliary visits and police surveillance on any ground other than privacy – a right which they referred to in theory but held not to be a part of the Constitution. The Court also held that the decisions subsequent to Kharak Singh upholding the right to privacy were to be read subject to the principles laid down in the judgment.

The Court also analysed the affirmative case for whether the right to privacy was protected under the right to life, personal liberty and the freedoms guaranteed under Part III of the Constitution. The Bench established that privacy was "not an elitist construct". It rejected the argument of the Attorney General that the right to privacy must be forsaken in the interest of welfare entitlements provided by the state.

Significantly, while holding that the right to privacy was not absolute in nature, the judgment also gave an overview of the standard of judicial review that must be applied in cases of intrusion by the State in the privacy of an individual. It held that the right to privacy may be restricted where such invasion meets the three-fold requirement of

1. legality, which postulates the existence of law;
2. need, defined in terms of a legitimate state aim; and
3. proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

Justice S.K Kaul added a fourth prong to this test which mandated "procedural guarantees against abuse of such interference".

At the same time, Justice J. Chelameswar held that the standard of "compelling state interest" was only to be used in privacy claims which deserve "strict scrutiny". As for other privacy claims, he held that the just, fair and reasonable standard under Article 21 would apply. According to his judgment, the application of the "compelling state interest" standard would depend on the context of the case.

The Court also emphasised the fact that sexual orientation was an essential facet of privacy. It further discussed the negative and positive content of the right to privacy, where the State was not only restrained from committing an intrusion upon the right but was also obligated to take necessary measures to protect the privacy of an individual.

The judgment held informational privacy to be a part of the right to privacy. The Court while noting the need for a data protection law left it in the domain of Parliament to legislate on the subject.

 ISSN: 2582-6433

4.3 PRIVACY IN RESPECT TO SEARCH & SEIZURE

M. P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi and Ors[150], in this case, the concept of right to privacy was first brought before the hon'ble court. The petitioner challenged the warrant for search and seizure issued by the authority under section 94 and 96(1) of the Criminal Procedure Code, 1973 as voilative to the fundamental right to privacy under article 21 of the Indian constitution. The Hon'ble Supreme court rejected the petition and denied to give reorganization to the right to privacy by stating that, the right to privacy is not an expressly incorporated Fundamental Right as it was not included in the constitution exclusively by the framers of the Indian constitution.

Kharak Singh v. State of Uttar Pradesh and Ors[151], in this case, the power of surveillance by the domiciliary visit of police at night was challenged by the petitioner as the violation of right to privacy under Article 21 of the constitution. The Court held that the surveillance by domiciliary visit is an intrusion and in fact is in contravention to Article 21 of the constitution. The court further stated that the right to privacy is not expressly provided under Article 21 hence, it does not form its part. Hence while delivering the dissenting judgement *Justice Subha Rao* was of the view that, although the fundamental rights does not include right to privacy as an exclusive right but it is an essential element of personal liberty under Article 21.

Gobind v. State of M.P[152], in this case the power of the police to domiciliary visit for surveillance was challenged by the petitioner as it was against the right to privacy under the Article 21 of the constitution. The hon'ble Supreme Court in this case upheld the validity of the right to privacy under article 21 by stating that the power of the police to visit a person's house or any place of residence at any time of day or night is contravene to right to privacy under Article 21. The court also referred that 'right to privacy' has to go through a series of cases as a process to become an absolute right.

4.4 PRIVACY IN PUBLICATION BY PRINT OR ELECTRONIC MEDIA

R. Rajagopal v. State of Tamil Nadu[153], this case is also known as '*Auto Shankar Case'*, the Hon'ble court in this case entertained the petition challenging the 'right to publication' as violation of right to privacy of a prisoner under Article 21 of the constitution. Supreme Court on

[150] (1954) SCR 1077
[151] (1964) 1 SCR 334
[152] AIR 1975 SC 1378
[153] (1994) 6 SCC 632

 ISSN: 2582-6433

this contention gave its verdict by declaring the 'right to privacy' as fundamental right guaranteed under Article 21and Article 19(2) of the constitution. The court further held that every person has an independent right to protect its privacy of his own, his family and marriage, motherhood, child bearing, etc; And any individual publishing anything related to any person public or private without his consent causes damage to the 'privacy rights' of that person and will be held liable for the damages.

Determining the gravity of the need of the 'Privacy rights' the court also took the initiative to lay down some specific ground on which the right to privacy can be claimed by the citizens. These grounds are:

a. No publication of 'name' of any female, who is victim of any offence such as 'sexual harassment, rape, kidnapping, abduction, etc.' shall be made in any media or press as it may harm the integrity of the female and violates the 'Decency' a reasonable restriction under Article 19(2).

b. Right to privacy shall not be available to the public officials in the situations where the matter is related to their discharge of power.

The court after determining the grounds at which privacy can be claimed also determined some of the exceptions under which the privacy cannot be claimed against any publication. These exceptions include:

a. Publication of court records

b. Publication in interest of public

c. Publication of public records

District registrar and collector v. Canara Bank[154], the apex court stated that tin the interest of the decency Art 19(2) an exception must be carved out from this rule namely, a women who is victim of an sexual assault, kidnapping, abduction or like offence should not further be subject

[154] (2005) 1 SCC 496

 ISSN: 2582-6433

to the indignity of her name and the incident being published in media.

State of Maharashtra v. Sanghraj Damodar[155] in this case, the hon'ble Supreme court held that the freedom of speech and expression which is present under Article 19(1) (a) which provides the police with power to 'seize the copies of the books, newspapers, documents etc.' and to search the places where they are reasonably suspected to be found is an invasion of the persons privacy.

State v. Charulata joshi[156], in this case the apex court held that the fundamental freedom of speech and expression under Article 19(1) (a) includes the freedom of press. This freedom is not considered as an absolute freedom. The court further held that the press must firstly obtain the consent of the person which it sought to interview and if the person who is sought to be interviewed has expressed his unwillingness then no court shall pass any order.

Sharda v. Dharampal[157], in this case the apex court held that the right to privacy under Article 21 is not a right in absolute sense. Court further held that if any conflict arises between the fundamental rights of two individual parties then the right which promotes the public morality will prevail.

Malak Singh v. State of Punjab and Haryana[158], in this case a petition was filed by the petitioner seeking the removal of his name from the register of surveillance which was maintained by the police station of the said jurisdiction under the guidelines of the Punjab Police Rules. The apex court upheld the validity of the police rules and said that the said surveillance must be conducted by the rules itself and not in the arbitrary exercise of its power.

Ram jethmalani v. Union of India[159], in this case the apex court elaborately dealt with the importance of 'right to privacy' and court stated that, the right of privacy is of utmost importance and is enjoyed constitutional right. It is important that the individuals must be granted such domains of freedom which are in manner free from the interference of the government until and unless the person acts in an unlawful manner. The court further held that the concept of the fundamental rights under part III of the constitution such as right to privacy is not such that the state is enjoined from derogating from them. It is the responsibility of the state to uphold them

[155] (2010) 7 SCC 398
[156] (1999) 4 SCC 65
[157] (2003) 4 SCC 493: AIR 2003 SC 3450
[158] (1981) 1 SCC 420
[159] (2011) 8 SCC 1

 ISSN: 2582-6433

against the actions of others in the society, even in the context of exercise of fundamental rights by those others.

4.5 PRIVACY IN PRIVATE AFFAIRS

State of Maharashtra v. Madhulkar Narain[160], in this case a police officer forcefully entered the house of women wearing his uniform. He asked her to have sexual intercourse with him but the women refused to do so. On her rejection the police officer forcefully tried to have intercourse to which she created a huge hue and cry. The matter went to court and police officer contented that the women is of easy virtue so the evidences produced by her should not be relied upon. The Supreme Court rejected the plea of police officer and held him liable for the breach of privacy of the women.

B.K Parthasarathi v. State of A.P[161], the individual's right to decide to have an intercourse is a very personal right of the individual. Additionally, this right also includes the 'right not to have an intercourse'. The invasion of the government in such decision making procedure of the individual was examined by the court in this case.

State of Punjab v. Baldev Singh[162], in this case Supreme Court held that women are meant to be treated with proper decency and dignity of which privacy is an essential part so not only the women of prevailing society but the prostitutes are also entitled to dignity, decency and privacy.

Rajinder v. State of Himachal Pradesh[163], in this case the court held that the person who commits crime of rape does not only breach the privacy of the victim but also the personal integrity of the individual. Offence of rape against a woman is not only the assault but it destructs the complete personality of the victim.

4.6 PRIVACY IN MARITAL AFFAIRS

Sareetha v. Venkata Subbaiah[164], in this case the A.P High Court has held section 9 of Hindu Marriage Act 1955 as unconstitutional because they were violative of Article 21 and right

[160] AIR 1991 SC 207
[161] AIR (2000) AP 156
[162] AIR 1999 SC 2378
[163] (2009) 16 SCC 69
[164] AIR 1983 AP 346

 ISSN: 2582-6433

to privacy embodied there in.

Harvinder Kaur v. Harmander Singh[165], the Delhi High Court neglecting the view of A.P High Court in above case, held that section.9 of the Hindu Marriage Act 1955 as valid. Court was of the view that although sexual intercourse is very subject of individual's privacy and it can only be considered as an essential element of the marriage but it alone does not constitute the whole marriage as it is not the only component of valid marriage. The same view of the Delhi high Court was upheld in case *Saroj Rani v. Sudarshan Kumar.*[166]

4.7 PRIVACY IN MEDICAL EXAMINATIONS

Mr 'X' v. Hospital 'Z'[167], in this case a government servant was suffering from a disease for which cure he was referred to the 'Z' Hospital in madras. The petitioner was directed by the government to accompany the sick govt. servant to the hospital at madras. On pursuance of the treatment there was the requirement of blood to which, the hospital authorities asked the petitioner to donate blood. On collection of samples of blood from petitioner it came out that he himself was HIV Positive and this information was somehow conveyed to the petitioner's would-be wife. As a result of such disclosure the marriage of the petitioner was called off and the petitioner sued the hospital authorities on the ground that they have failed to keep up their patient-doctor ethics and breached his right to privacy under Article 21.

Hon'ble Supreme Court in this case held that the disclosure of the information by the hospital authorities about his illness is not violation of right to privacy under Article 21. The court further held that although privacy is a fundamental right but is not in its exclusive sense absolute and this right is subject to the several restrictions. As marriage under every matrimonial law is said to be not a valid marriage if spouse is suffering from a vulnerable disease which is of incurable nature. So the disclosure of petitioners information of his disease is not breach of his right to privacy because disclosure of such information has saved the life of the girl with whom petitioner was about to get married.

Selvi v. State of Karnataka[168] in this case the Hon'ble Supreme court of India has held that the medical examinations like 'Narco Analysis' and 'Lie detection test' if conducted on a

[165] AIR 1984 Del. 66
[166] AIR 1984 SC 1562
[167] AIR 1991 SC 207
[168] (2010) 7 SCC 283

 ISSN: 2582-6433

person in a forced way without the prescribed conditions is said to be the violative of 'Right to Privacy' of an individual.

Bhabani Prasad Jena v. Orissa State Commission for Women[169], in this case the court held that if in any circumstances the performance of DNA test is essential to reach the truth, then even if its performance is violative of persons privacy the court shall conduct it because of the reason that it is not an absolute right.

Ms. 'X' v. Mr. 'Z'[170], in this case a husband accused her wife of having an adulterous relation with another man which has resulted in her pregnancy. The abortion was done at AIIMS and the foetus was preserved by the hospital itself. The husband filed an application to the court seeking to allow DNA testing of the foetus to ascertain that if he was the father of that foetus or not. This contention of husband was pleaded by wife as a violation of her privacy. To this Hon'ble Court held that, the request of husband to seek a DNA test is not violation of wife's right to privacy as the foetus is already being discharged from her body and no longer her part and it preserved by the AIIMS itself.

Neera Mathur v. LIC of India[171], in this case the Hon'ble Supreme Court of India held that open disclosure of the problems such as 'her menstrual cycle is regular or not' is also an breach of her modesty and privacy.

4.8 RIGHT TO PRIVACY IN EXAMINATION OF VIRGINITY

Surjit Singh Thind v. Kanwaljit Kaur[172], in this case the wife filed a petition for decree of nullity of her marriage on the grounds that her husband is an impotent and their marriage was never consummated. The husband in his argument asked the court to issue the medical examination of her wife to determine the fact that she is not a virgin and he is not an impotent and their marriage was completely consummated. The court held that, issuing of such an order to conduct the medical examination of a women to determine her virginity is complete violation of her privacy rights embodied in Article 21 of the constitution.

4.9 PRIVACY IN TELEPHONE TAPPING

[169] (2010) 8 SCC 633
[170] AIR 2002 Del. 217
[171] AIR 1992 SC 392
[172] AIR 2003 P&H 353

 ISSN: 2582-6433

Amar Singh v. Union of India[173] in this case apex court held that the regularity in official communications must be maintained when in such matters the network provider is taking serious steps to capture the phone conversations and by doing so these service providers are intruding the privacy of the concerned individual. The court further held that it is the duty of the service providers that they should act more carefully and responsibly.

Rayala M. Bhuvaneswari v. Nagaphamender Rayala[174], in this case a husband tapped the conversations of his wife with her family and friend in order to produce before the court as an evidence for obtaining a divorce decree. The court in this case held that, the husband's act of tapping his wife's telephonic conversations without her consent is the violation of wife's 'Right to Privacy' and those recordings cannot made admissible to the court as an valid evidence.

RM Malkani v. State of Maharashtra[175], in this case the apex court held that the court will not entertain the safeguards for security of then resident of the country to be infringed by granting permission to the police to inquire in to matters by illegal methods. The telephone tapping is the direct interference and infringement of individual right to privacy and freedom of speech and expression. The court also stated that the government cannot force prior restrictions on publication of the defamatory materials against its servants, if it does so then it would violate the article 21 and article 19.

N.C.T of Delhi v. Navjot Sandhu @ Afsan Guru[176], in this case the apex court held that under the statutes of special nature such as POTA the required conditions for admitting the evidence against the accused through the capturing of wire, electronic or oral communication have to be compiled with before accepting such material as an evidence in the court.

People's Union for Civil Liberties (P.U.C.L) v. Union of India[177], popularly known as the *'phone tapping case'.* in this case P.U.C.L a voluntary organization filed a writ petition under Article 32 of the constitution. The petition challenged the validity of the section 5 of the Indian Telegraph Act, 1885. The said section provided the state and central government power to tap the phones in the certain listed circumstances. The petition filed was in via of the phone tapping of

[173] (2011) 7 SCC 69
[174] AIR 2008 AP 98
[175] AIR 1973 157
[176] Appeal (CRl.) 373-375, 2004
[177] AIR 1997 SC 568

 ISSN: 2582-6433

the politicians by the C.B.I.

The matter considered by the court as an unpleasant event as the law does not provide any of the preventive measures that could be taken to prevent the misuse of the power provided by section 5 of the said Act. The court said that though the state and the centre governments are provided with such a discretionary power but it must only be used by the Authorities in the occurrence of following events:

- In the event of public emergency
- In the event where the matter is of public interest
- In the event where sovereignty and integrity of the nation is at stake
- In events where security of state is involved
- In events where matter is related to relations with friendly states.

The court further laid down the procedural safeguards in order to prevent intrusion of one's privacy by the state authorities:

1) An order for tapping a phone must only be issued by the Home secretary of the State or Centre but in the case of an emergency situation it can be delegated to an officer of Home Department of state or center who is not below the rank of Joint Secretary.

2) Once the order is passed its copy is to be send to the Review committee within the week of the order released.

3) The order issued must operate for the time period of two months. It can be reviewed by the committee and the time of operation can be extended.

4) The individual issuing the order shall keep the records of, communication, no of individuals and their identity to whom such matter is to be disclosed in front of the authority.

5) The use of the material shall be restricted to the low as possible that is important in terms of the said provision.

 ISSN: 2582-6433

6) The committee shall on its own within three months inquire wether there is relevant section under the provision.

7) The review committee stated that there has been violation of said section, shall set aside by the order of the authority. It can also direct the disruption of the copies of material.

8) If on inquiry the committee comes to the result that there has been no intravention of the section it must record its finding.

The judgement of the apex court delivered by the bench of two judges who opined that, with the development of the communication technology the right to privacy to hold conversation on telephone is increasingly misused in the society. The court's ruling laying some detailed guidelines for the authority for implementation of the provision under the Act. By preserving the right to privacy the Apex court enhanced the scope of Article 21 under the Indian constitution.

4.10 GOVERNMENT INTERFERENCE IN RIGHT TO PRIVACY

Unique Identification Authority of India v. Central bureau of investigation (2014) in this case the CBI access to the bulk of the data base complied by the unique identity authority of India for the examination of a criminal offence the apex court held that the UIDAI was restricted to transfer any bio metrical information without the individual consent the ruling has importance for the governmental biometric ID scheme, covering excess to bank account and payment of taxes etc the data of a concerned individual could be misused the authorities stated that the registration to be compulsory the verdict overruled the previous two ruling by the apex court which stated that the privacy is not included in part III of the constitution.

4.11 PRIVACY OF DATA

Bhim Sen Garg v. State of Rajasthan[178], in this case it was held that, fabrication of an electronic record or committing forgery by way of interpolations in CD produced in a court as an evidence attracts punishment under section 65 of the Information Technology Act 2000.

[178] (2006) Cri LJ 3463

 ISSN: 2582-6433

Rajkot Municipal Corporation v. Manjulben Jayantilal Nakum[179], the court in this case held that, the object of the law is not always to provide compensation for all the losses that may occur. If such object is aimed then it will be overambitious and will conflict with the basic concepts of the social policy. Society has no interest in mere shifting of losses between the individuals for its own sake. The loss by hypothesis may have already occurred and whatever benefit might be derived from repairing the fortunes of one person is exactly offset by the harm caused through taking that amount away from another. The economic assets of the community do not increase and expense is incurred in the process of realization. The court further observed that, the common law principles evolved in England may be applied in Indian context if there is the absence of the statutory laws in India.

Shri Umashankar v. Sivasubramanian ICICI bank[180], the adjudicating officer granted the compensation of rs.12 lakhs to the petitioner. In this case the court held that the ICICI bank has failed to establish the due diligence which was exercised to avoid the confliction of nature of unauthorized access as laid under section 43 of the I.T Act 2000. It was also held that bank has failed to provide the complete internet banking system with established authentication and validation which would have prevented the unauthorized access which led to great financial loss to the petitioner.

Pooja Chandrakant Darooka v. Sri Nainesh Modi[181]; the crime relating to the fraudulent credit card and debit card transactions was confessed by the offenders before the adjudicating officer, Gujarat. The court ordered the offenders to pay ten instalments of rs.8500 each to the petitioner totally amounting to rs.85000.

JCB India ltd. v. Abhinav Gupta[182], in this case an ex-employee was accused of data theft and copyright violations by the petitioner. The adjudicating officer in this case dismissed the petition on the grounds of the 'lack of jurisdiction'.

Parimal Manharlal patel v. Dena Bank[183]*;* in this case the Adjudicating Officer of Gujarat declared the banks namely Dena Bank, Standard Chartered Bank, Axis Bank as innocent from the negligence. The Officer further held the Idea Cellular Ltd. as liable for issuing the duplicate

[179] (1997) 9 SCC 552
[180](2010) 10 SCC 789
[181] (2011) 1 SCC 756
[182] (2010) 4 SCC 598
[183] AIR 2016 SC 654

 ISSN: 2582-6433

SIM without verification of the customers.

State of Maharashtra v. Marwanjee F. Desai[184], hon'ble Supreme Court in this case held that the authorities 'power to summon the witness and force its attendance, examine them while on oath or directing for production of the documents or records' depicts the quasi judicial feature of the proceeding.

Bharat Bank Ltd v. Employees of Bharat Ltd, Delhi[185], in this case it was held by the Apex court that the constitute a court in a strict sense , it must have an essential condition that apart from the trappings of the judicial tribunal it must have the power to give the binding decision which should have some definite authoritativeness.

Trimex International FZE Ltd. v. Vedanta Aluminium Ltd[186], in this case the apex court held that in the case where a duly signed agreement is absent between the parties it could be confirmed by the duly approved and signed documents in the form of e-mails, letters, telex, or any other means of communication.

4.12 PRIVACY IN COMPUTER RELATED OFFENCES

Abhinav v. State of Haryana[187], in this case the court has explained the term 'Hacker' and 'Hacking' in a elaborative sense. The court said that, a hacker is an individual whose criminal intention persuades him to break in to a computer system. Hacking is a computer trespass. To constitute hacking into an offence there should be the element of mens rea present in it. Court further divided the two categories of the hackers i.e.

(i) Hackers who do not intent to break in to an computer system to cause the harm. They are also referred as 'white-collar-hackers' as the hacking done by them is not not considered as a criminal activity.

(ii) The second category are the 'crackers' means the hackers who are having an evil intention to break into someone's computer system and cause some harm to them. This sort of hacking is a crime under the law.

[184] (2002) 2 SCC 318
[185] AIR 1950 SC 188
[186] (2010) 3 SCC 1
[187] AIR 2008 SC 1956

 ISSN: 2582-6433

Dr.Vimla v. Delhi Administration[188], in this case the hon'ble court held that the judicial position of the expression 'dishonestly' and ' Fraudulently' which are used under the various provisions of the said statute indicates that these two terms are so closely related to each other that definition of the one term may give colour to the other term.

Shreya Singhal v. Union of India[189], this case is considered to be a very important case in the constitutionality of the various provisions of the Information Technology Act 2000. In this case ; at the death of the Shiv Sena Leader Sri. Bal Thakerey there was a comment posted on asocial media platform by two girls, one posted the comment and other liked the comment. The Bombay police arrested those two girls under section 66A of the Information Technology Act 2000. The following issues were raised in this case before the Apex Court:

(i) The constitutional validity of section 66A of the said I.T Act 2000

(ii) Whether this section is infringing the freedom of speech and expression

(iii) Whether the said section is protected under the Article 19(2) of the constitution.

The court considering the issues in this case held that, the said section i.e. Section 66A of the I.T. Act 200 is unconstitutional on the ground that it takes away the protected speech which is innocent in nature and is liable to be used I such a way as to have a cooling effect on the speech in free sense. The court further struck down the section 66A as unconstitutional as it is violative of Article 19(1) (a) and is not saved under the Article 19 (2) by giving the reason that the provisions which have the vague meaning must be struck down immediately because such provision will further mislead the administrators and will also cause the harm to the people in a social order. The court further showed its intolerance for arbitrary provisions by stating the 'the statute can have sometimes the loopholes but never a vague provision'.

Aveek Sarkar v. State of West Bengal[190], in this case the hon'ble cour laid down the test for determination of the obscene information. Court held, 'infirmation which is so posted in an context or in a background which consequentially effects or outrage the modesty of the individual as pictured.

[188] AIR 1963 SC 1572
[189] WP (CRl.) No. 167 of 2012
[190] (2014) 4SCC 257

 ISSN: 2582-6433

State of Madhya Pradesh v. Baldeo Prasad[191], in this case, an inclusive definition of the term 'goonda' under the Goondas Act was held invalid and the offence created by the section 4A under the said Act was therefore held violative of Article 19(1) of the constitution.

K.A Abbas v. Union of India[192], in this case the petitioner challenged the pre-censorship of movies as violation of freedom of speech and expression. The court in this case held it valid and is as not violative of Article 19(1).

Sanjay Jha v. State of Chattisgarh[193], in this case the court defined the term 'identity theft'. The court stated that the offence of 'identity theft' is said to be committed when by means of fraud or dishonestly one does the downloading, copying, extraction of electronic signature, passwords or any unique ID etc, with the criminal intention to cause loss or harm to the victim. The court in this case denied the bail to the accused because he was under the serious offence of illegally duplicating the letter head of the Railway Minister.

Bennet Coleman v. Union of India[194], in this case the apex court held that the term "publication" means printing and circulation. In the context of the internet publication, the term may include dissemination, storage and transmission of data or information in any electronic form.

Banu Tamta v. High Court of Delhi[195], this case the apex court gave birth to the 'The Gender Sensitisation & Sexual Harassment of Women at the Supreme Court of India (Prevention, Prohibition, and Redressal) Regulations 2013".

Court on its Motion v. State[196],in this case the hon'ble High Court of Delhi held that no 'sting operation' can be done in order to induce any person to commit any crime. The sting operation before its performance must be sanctioned by an appropriate authority. Court further stated that though in India there is absence of any such authority then in such a case until and unless on is established by the law any sting operation by any private individual or by any agency must be sanctioned by the court of that competent jurisdiction because it is essential to ensure the legal limits over any such activity which is potentially qualified to destruct the privacy of an

[191] (1961) 1 SCR 970
[192] (1971) 2 SCR 446
[193] (2014) 3 SCC 202
[194] (1972) 2 SCC 788
[195] WP (C) 162 of 2013
[196] WP (CRL) No. 796/2007

 ISSN: 2582-6433

individual.

Avnish Bajaj v. State[197],in this case a registered seller on the online sale-purchase portal uploaded a MMS clip for sale on the website. The seller in order to hide its identity from being traced put the registration names and credentials fake. The pornographic material as was prohibited to sell on such portal was removed within 24 hours from the web portal. In those 24 hours 8 people purchased that clip from different states. On the aggravation of the matter the Crime Branch Delhi started the investigation and arrested the seller on 17th December 2004. The court in this case referred to the judgement of 'Shreya Singhal case' and held that, "not having the concerned filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, that the website ran a risk of having gained it the knowledge that such object was in fact obscene and thus it can be held that as per the strict liability imposed by section 292, knowledge of the listing can be imputed to the company."

Dr. V. Prakash v. State of Tamil Nadu[198], in this case the apex court dismissed the petition as the court could not find any merit in the plea that the any prejudice is caused to the petitioner because of the delay of two days in furnishing the translated copies of the documents. It was further held that the letter received from the member public were not irrelevant.

Mohammed v. State[199], in this case the court analyzed the section 67 of the Information Technology Act 2000. The court held that this section is not applicable to the case of threatening email received by the Chief Minister of Gujarat and hence ordered to be deleted from the context.

Sreekanth C.Nair v Licensee/developer[200], in this case a student of ASCL, found a website namely www.incometaxpune.com which on opening redirected to the pornographic site. The petitioner moved to the court for seeking an order to block the website. The court in this case ordered that the petitioner can only move to the court only when the said authorities established under I.T Act are first visited and the authorities had refused to entertain the complaint.

Christian Louboutin SAS v. Nakul Bajaj [201], in this case the court greatly analyzed the section 79 of the information Technology Act. The court also laid down the circumstances in

[197] AIR 2008 SC 673
[198] (2002) 7 SCC 759
[199] AIR 2010 SC 639
[200] AIR 2008 SC 295
[201] (2018) 9 SCC 496

 ISSN: 2582-6433

which the portal intermediary will be seen as to be the abettor in selling of online products and services. Therefore, the court declared that even if the middle-men has the understanding of the unlawful activities happening over their website then the intermediary does not need the order of the court to stop the counterfeited products from using the service of the intermediary. If the operation of using the intermediary services continues even after the minimum knowledge to intermediary then the intermediary will be held liable.

Petronet LNG v. Indian Petro Group[202], in this case Delhi High Court held that the companies and the established corporation cannot assert the fundamental right to privacy. Further in this case court held that the right to privacy is not exclusively available against the non-state individuals.

4.13 FREEDOM TO INFORMATION

Girish Ramchandra Deshpande v. Central Information Commissioner[203], in this case the question before the apex court was whether matters pertaining to an individual's service career and details of his assets and liabilities, moveable and immovable properties etc. can be treated as personal information as defined under section 8(1) (j) of the Right to Information Act 2005. The Apex Court held that the performance of an employee in an organization is a matter between the employer and the employee; and the particulars called for by the petitioner including show-cause notice and orders of punishment, fall under the ambit of personal information. Details disclosed under the income tax returns are also to be treated similarly.

Mr. Surupsingh Hrya Naik v. State of Maharashtra through Additional Secretary, General Administration Department[204], the court in this case held that, confidentiality that is required to be maintained by the medical records of the patient, including a convict, considering the Indian Medical Council Regulations 2002 cannot override the provisions of the RTI Act. The court further held that if there is inconsistency between the regulations and the RTI Act then the provisions of the RTI Act will prevail. The Act carves out some exceptions, including the release of the personal information of the disclosure of which would amount to the invaision of the privacy.

[202] AIR 2009 SC 163
[203] AIR 2012 SC 362
[204] AIR 2007 Bom. 121

 ISSN: 2582-6433

Subhash Chandra Aggarwal v. The registrar, Supreme Court of India[205], in this case the question before the Delhi High Court was regarding the disclosure of information including the details of medical facilities availed by individual judges. The court in this case considered the fact that the total expenditure incurred for the medical treatment of the judges for the period in question was already being furnished by the Central Public Information Officer and it is not the case of the appellant that the said expenditure is excessive. The court further held that the details of the medical facilities availed is the personal information and there is no public interest warranting the disclosure of the same.

Public Information Officer v. Andhra Pradesh Information Commissioner[206], in this case an overview of the laws pertaining to the RTI Act, especially section 6 to 8 was given. These sections give the impression that the legislature has tried to harmonize the conflicting public and private rights and interests by building the sufficient safeguards. The court further stated that, this is the reason why section 8, when applied should be given a strict interpretation as it is a fatter on not only a statutory right under RTI Act but also a pre existing constitutional right.

Bhagat Singh v. Chief Information Commissioner[207], the court held that as the argument seems logical and as appropriate in several circumstances, it does present a problem when dealing with the privacy exception contained in section 8(1) (j). This is because the privacy traced in this provision is also found in some provisions of the constitution from which the constitutional right of freedom of information emerge i.e. Article 14, 19(1) (a), and Article 21 of the constitution.

4.14 RECENT DEVELOPMENTS

Karmanya Singh Sareen v. Union of India[208]*(Whatsapp privacy policy case)*,a petition is filed in the Supreme Court challenging the 'whatsapp' privacy policy change allowing sharing of data with the 'Facebook'. The policy was first challenged in the Delhi High Court by petitioners who claimed violation of user's privacy. In September the Delhi High Court had ruled that Whatsapp had to delete user account information of all those who deleted the application and that the company could not share such information with its parent company 'Facebook' up to the date of the order. The petition specifically points out the government's responsibility to guarantee and ensure the protection of the personal and private data when using such modes of communication

[205] AIR 2015 SC 1567
[206] AIR 2009 AP 459
[207] AIR 2008 DLT 385
[208] W.P. (C) 7663/2016

 ISSN: 2582-6433

whereby private and confidential data and information is exchanged.

The department of Telecommunications informed the court that the top social media platforms such as Whatsapp, Facebook, and Skype were sought to be covered by new regulations that are being explored. This marks the significance of the new privacy legislation that are sought to be introduced soon in addition to available current legal framework provided by the Information Technology Act and complemented by the other available general laws. Earlier concerns relating to the review and passage of the new Privacy Bill, due to reservations from various quarters, are sought to be addresses soon.

Justice K.S Puttaswamy (Retd.) v. Union of India[209], in this case the 'Aadhaar Card Scheme' was challenged on the ground that collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is in breach of the fundamental right to privacy embodied in Article 21 of the Constitution of India. Given the ambiguity from prior judicial precedents on the constitutional status of the right to privacy, the Hon'ble Supreme Court referred the matter to a constitutional bench consisting of nine judges.

It was argued on behalf of the Petitioners that the right to privacy is very much a fundamental right which is co-terminus with the liberty and dignity of the individual and this right is found in Articles 14, 19, 20, 21 and 25 of the Constitution of India read with several international covenants. On the contrary, the Union of India contended that 'right to privacy' is not a fundamental right guaranteed under the Constitution. The primary defence of the Union of India was that:

(i) If the framers of the Constitution wanted to include the 'right to privacy' as a fundamental right, the same would have been specifically included within the Constitution;

(ii) Privacy is inherently a subjective and vague concept. The concept of privacy is difficult to define. Such vague concept cannot be elevated to a fundamental right;

(iii)The present laws already confer sufficient protection to individuals against the invasion of privacy; and

[209] (2015) 8 SCC 735

 ISSN: 2582-6433

(iv) 'Right to privacy' is a legitimate claim having the sanction of common law, each such claim cannot be elevated to a fundamental right.

The Hon'ble Supreme Court by its decision pronounced on August 24, 2017, unanimously held as under:

a) The decision in M P Sharma which holds that the right to privacy is not protected by the Constitution stands over-ruled;

b) The decision in Kharak Singh to the extent that it holds that the right to privacy is not protected by the Constitution stands over-ruled;

c) The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

d) Decisions subsequent to Kharak Singh which have enunciated the position in (c) above lay down the correct position in law.

Justice D.Y. Chandrachud[210], clearly held that: -

A. Life and private freedom are freedoms that are inalienable. These are rights that cannot be separated from a dignified natural life. Individual dignity, human equality and the quest for freedom are the cornerstones of the Indian Constitution;

B. Privacy is a constitutionally protected right that arises in Article 21 of the Constitution mainly from the guarantee of life and personal freedom. Privacy aspects also emerge from the other manifestations of liberty and dignity recognized and secured by the fundamental rights provided in Part III in different situations;

C. Privacy involves preserving private intimacy, the sanctity of family life, marriage, procreation, house and sexual orientation at its heart. Privacy also means being left alone. Privacy protects the autonomy of individuals and acknowledges the individual's capacity to regulate essential elements of their lives. Privacy is inherent to personal decisions regulating a manner of life. Privacy safeguards heterogeneity and recognizes our culture's plurality and diversity. While lawful privacy expectations may differ from intimate area

[210] *Supra note 223 at p 93*

 ISSN: 2582-6433

to personal area and from personal to government forums, it is essential to emphasize that privacy is not wasted or abandoned simply because the person is in a government location.

Privacy attaches to the person since it is an essential facet of the dignity of the human being;Like other rights that are component of the basic liberties guaranteed under Part III, including the right to life and freedom under Article 21, privacy is not an utter right. A law that infringes privacy will have to resist the touchstone of allowable fundamental rights constraints. An invasion of privacy must be justified in the context of Article 21 on the basis of a law stipulating a fair, fair and reasonable procedure. The legislation must also be applicable in relation to the invasion of lives and private freedom pursuant to Article 21. An invasion of human life or personal freedom must comply with the three-fold requirement of (I) Legality that presupposes the law's existence, (ii) Need that was described in a legitimate state objective and (iii) Reasonableness that provides for a rational connection between the objects and the means to them, and the substance of privacy is positive as well as negative. The adverse material restricts the state from intruding into a citizen's lives and personal freedom. Its favourable material enforces on the state an duty to take all needed steps to safeguard the individual's privacy[211].

While evaluating the essence of the right to privacy in respect of its origins, the Court of Justice dismissed the Union of India's statements and ruled that the right to privacy is inherent and inseparable from the human element and root of human dignity. It was therefore maintained that the meaning of privacy is both good and bad. The adverse material functions as an obstacle to the state's interference with the lives and personal freedom of its citizens and its favourable material requires the state to adopt all steps needed to safeguard the privacy of the person. The statutory privacy security can consequently result in two interrelationship laws i.e. (i) against the whole world that all states, including: the right to choose what private data should be disclosed to the public domain (ii) against the State: democratic values combined, limiting the administration and limiting the authority of the State as needed.

The right to privacy has become, as a consequence of this judgement,' more than pure common law' and' more solid and sacrosanct' than any statutory right. Thus, an infringement of privacy must now be performed in the framework of Article 21 of the Constitution on the grounds of' a law' which stipulates a fair, honest and sensible operation. It's worth noting that since R.C. Cooper v Union of India,' law-established operation' in Article 21 has acquired substantive due

[211] *Supra note 223 at p. 93*

 ISSN: 2582-6433

process component and even the contents of the law may be questioned because they do not comply with the demands of a valid law. Consequently, given that the right to privacy is recognized as a fundamental right, existing territorial legislation may now have to pass the rigors of the aforementioned test if it is called into question. If privacy stayed merely a statutory or common law right, the same would not have been the stance.

In debating today's world's right to information protection, Justice D.Y. Chandrachud stated as follows:-"Information privacy is a facet of privacy rights. In a data era, the risks to privacy can come not only from the government, but also from non-state performers. We commend the need to examine and implement a robust data protection regime for the Union government. Establishing such a system needs a cautious and delicate equilibrium between personal interests and the state's rightful issues. For example, the state's lawful goals would include maintaining national security, stopping and researching crime, promoting innovation and information dissemination, and preventing social welfare benefits from being dissipated. These are policy issues that the state of the Union must consider while developing a closely organized data protection system. Since the govt of the Union has notified the Court that it has established a committee headed by the former judge of this Court, Shri Justice B.N. Srikrishna, the issue shall be dealt with properly by the government of the Union having due consideration to what has been set out in this judgement.

We're in an era of data. More information is now easily available with technology growth and development. There are many benefits to the information explosion, but also some disadvantages. Access to information that an person may not want to provide requirements privacy security. Recognition and enforcement of claims by non-state actors may require the State to intervene legally. The right of privacy shall be asserted qua State actors and non-state actors.[212]"

4.15 CONCLUSION

The researcher in this chapter has studied the approach of the Indian Judicial system towards the Right to Privacy and the Data protection. Through the study it can be seen that the approach of Judiciary regarding Privacy as a fundamental right is positive as in many cases court have considered it as a essential right under the Part III of the Indian Constitution. As in the most latest development in the 'Aadhaar Case' the court held the Right to Privacy as an intrinsic part of the

[212] N.S. Ramnath, *The Adhar effects : why world's Largest Identity Matters* 84 (Oxford University Press, New Delhi, 2018)

 ISSN: 2582-6433

Article 21 of the Constitution in influence to which the legislature has also taken a step forward in concretizing the verdict and introduced the Data Protection Bill, 2018 in the parliament.

CHAPTER -FIVE

CONCLUSIONS AND SUGGESTIONS

After studying and analyzing the chapters of this research study, the summary is that in this Research the researcher has been investigating the concept of Privacy in India so far. The researcher in his research studied the deliberately what privacy is and what is its importance in the era of technological advancement where the information is a key actor. The study comprises of the introduction, research methodology, review of the literature, hypothesis, significance of the Right to Privacy and Data protection in India. Researcher has also studied the objectives behind the research conducted on the Privacy Right and Data Protection in India. The concept of privacy right is an essential right of the citizens and also the problem faced by this right in today's era of information and data. The researcher has further studied the overview of the Right to Privacy and Data Protection and given an elaborative explanation of the concept of privacy and some dictionary and scholarly definitions of privacy right. The roots or the origin of the privacy right and its development in different times and in different dimensions is also included in the research work.

Further in the research, the law's presently operating in India in regard to the privacy and the data protection are studied exclusively. All the constitutional provisions which are considered to be connected to the privacy specifically Article 19 and Article 21and all the different legislations like Information Technology Act, Hindu Marriage Act, Indian Penal Code, etc are taken into the consideration. The study also touches the several schemes and the expert

 ISSN: 2582-6433

committee's recommendations and the Draft Bills relating to Data Protection which are pending in the parliament waiting for the approval to become a law. Moreover, the social and legal effects of the privacy and data protection in Indian society are studied by the researcher. It deals with how society is connected to the information and what is the primary necessity of the accuracy of this information. The information is misused and how its misuse leads to several criminal activities like cyber crimes, identity thefts etc. Submissions and sharing of personal information on the social media platforms and how its deteriorating effects are tackled by law of the nation is also discussed.

Later in the research the prime focus is put on the approach of the Supreme Court regarding the right to privacy and protection of data. Also the recent developments towards the privacy as a fundamental right and discussions about present threat to privacy in the protection of data are highlighted.

5.1 CONCLUSIONS

The researcher after going through the all the materials in the above-studied chapters, have drawn the following conclusions:

1. Privacy is an individual's or group's ability to detach or uncover information about themselves specifically. The boundaries of what is perceived as personal vary between the cultures and individuals, yet they share basic topics. When something is private to an individual, it mostly implies that something is seen as intrinsically extraordinary.

2. The right of not being subject to the administration or individuals to unwanted attacks on data privacy is a piece of the protection legislation of various countries. Practically all nations have laws on privacy here and there; case of this would be tax assessment law, which regularly requires the sharing of personal wage or profit data.[213]

3. In today's global market, a person can deliberately supply his or her personal information for the advertising purposes, such information could be stolen or misused that could lead to identity theft or other cyber crimes.

[213] Gaurav Goel, *Right To Privacy In India: Concept & Evaluation* 26 (Partridge India, New Delhi, 2016)

 ISSN: 2582-6433

4. The privacy protection laws do not limit any general intrusion problem. Until now, the law that identifies with the right of protection has been consigned to a status which is still experiencing some difficulty in the early stage. There has already been a chance for the legislature and the information technology sector to look at the accessible funds to regulate the problem of privacy breakdown.

5. The protection of privacy and protection of one's personal data are the key human rights considered in the United Nations Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other colonies around the world. Privacy as a right promotes the other important characteristics, such as membership opportunities and freedom of speech.

6. The right to privacy and data protection reflects the evolving importance, assorted diversity, and multifaceted nature. It is due to the rise of data innovation which led the right of privacy under the real risk and the use of various electronic contraptions has made it extremely easy to recognize people's activities over the internet. It has been noted that the present regulations are inadequate to manage this problem, and this needs a fresh legislation to be introduced.[214]

7. In a significant number of countries where privacy is not seen in the Constitution, such as the United States, Ireland, and India, the judiciary have found that in various agreements immediately. Global understandings about perceiving privacy rights in many countries like United States, Ireland and India, the judiciary have found the privacy right as in separate agreements.

8. The global understandings recognizing the privacy freedoms have been incorporated into law in various countries, such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights. Nations began to embrace expansive laws to secure individual protection in the mid-1970s.

9. Recognizing both the shortcomings of law and the numerous distinctions in the dimension of privacy in each of the states, the European Union passed an order that would give indigenous people a wider range of assurances about their information being mistreated.

[214] Kiran Veshtak, *Right To Privacy Under Indian Law* 76 (Deep And Deep Publications, New Delhi, 2012)

 ISSN: 2582-6433

The order on Individual's assurance regarding the handling of individual data and the free creation of such data establishes a benchmark for domestic legislation.

10. The right to privacy could only be practiced if the offender is a government and not a private person or organization. This non-absolute right can tamper with public health norms and health concerns. This right does not prevent publishing matters of particular concern.

11. In India the predicted problem is that some sections in the Indian environment are to be managed but is, unfortunately far greater than the approval of sound protectionist legislation.

12. Distributed computing has critical ramifications to protect individual information as well as legislative data privacy. The main goal of this inquiry is to differentiate between protection and privacy issues that may be of primary concern or concern to members.

13. Numerous experts argue that distributed computing is safe than the various standard data storage methods, such as servers, and so on, but organizations still go for data breaches. The basic motive behind why cloud administrations are not chosen by organizations is the lack of privacy. In the Indian situation, the distributed computing is a new idea, there is no law that explicitly oversees it, and the law needs clarity at present. Inquiries concerning the relevant law and court ward remain unanswered.

14. Cyber crime courts, specialized judges with intellectual property jurisdiction and information privacy issues, are a needed answer to the regulatory problems faced by India. In addition to provide appropriate data security, and to retain its increasing presence in the worldwide computing sector, India should promptly embrace this scheme of specialized judiciary.

15. Except the Credit Information Companies Act 2005 includes privacy requirements that spread most periodic information assurance freedoms, but only in relation to loan announcement setting, there is generally no critical enactment that ensures individual data in India so far, but some sections in the Information Technology Amendment Act, 2008 may rise as heavy reliance on guidelines made and used, especially regarding data privacy.

 ISSN: 2582-6433

16. Specific standards concerning the techniques and purpose of assimilating private information offline and over the Internet need to be established in a legal framework.

17. A main criticism of the Draft Bill is that it aims at safeguarding information as an end in itself, not as a means to the end. Certainly, via discussions and recommendations, the Bill is probable to suffer important flipping, and it continues to be seen whether India strikes equilibrium among these two different interests. As Justice B.N. Srikrishna said, "This report is just like the purchase of new boots. It'll be narrow at first, but within a span of time it'll be convenient."

5.2 SUGGESTIONS

From the above study the following suggestions have been made by the researcher:

1. There must be a constitutional amendment which includes the Right to Privacy exclusively in the Part III of the Constitution.

2. There must be a comprehensive National Policy to ensure that individuals have the privilege of controlling their own information, collection and its transmission.

3. The following rights must be awarded to every individual in an explicit form: Right to restrict the accumulation of data, the exchange of data and the use of data; Right of accessing personal data and making corrections to it; Right to keep the Personal Data safe.

4. Internet based transactions must be maintained and the development of sophisticated mechanical and lawful provisions will clear the path for web security and data authentication.

5. There must be some reasonable restrictions which should be imposed on both state and private authorities regarding the use or collection of an individual's personal data.

6. The legislature must and without further delay should pass the Data Protection Bill which can bring some relief to the looting of data day by day.

 ISSN: 2582-6433

7. Legislative guidelines must be issued restricting the social media platforms from making such fraud policy user agreements that cause the breach of individual's personal information.

8. International trade has grown and have many consequences, particularly with the cyber impact, it is essential to collaborate with the global society to lay down legislation exclusively relating to privacy and private data security.

9. It is suggested that the online customers must take responsibility for their digital transactions and should be aware of the transactions and use appropriate security attempts to safeguard their privacy, for instance, encryption.

10. It is suggested that there must be a single legislation which must integrate sections dealing with the financial portion of the transactions and the relationship between an internet service provider and a third party, as it is essential to determine the violator's character.

11. There are scattered provisions in different laws relating to the privacy, these scattered provisions must be gathered around and put under the single head so as to provide a defined code for securing the privacy of a person under different cases and circumstances.

12. Cyber infringement courts are an important solution to Indian issues of data infringement, the special courts will deal with registered technology and data safety issues.

13. It is suggested that such a law should be made which provide a tool that would establish punishment against the violators and offer compensation to an abused person. In addition to this, the law must be applied to the administrative authorities also.

14. There is need to set up the more strict standards for the social media developers so that they could be prohibited from finding any sloppy ways of getting an illegal access and from misusing the personal information of a user.

15. It is suggested that the approach of the Indian judiciary must be more open and strong regarding Right to privacy and the data security, as it is the need of the hour.

 ISSN: 2582-6433

BIBILIOGRAPHY

1. BOOKS

Dash, Ajay — *Sting Operation by Media* (Eastern Book Company, New Delhi, 2007)

Westin, Alan F. — *Privacy and Freedom* 8 (Princeton University Press, New York, 1970)

Bennett , Colin John — *Policy Instruments in Global Perspective* (Princeton University Press, New York, 2003)

Basu, D.D. — *Law of the Press* (Universal Law Publishing, New Delhi, 2002)

Brien, David M.O — *Privacy Law and Public Policy* 64 (Praegor Publishers, America, 1979)

Niblett, G.B.F. — *Privacy and Human Rights* 73 (Oxford University Press, London, 1972)

Goyal, Gaurav — *The Right to Privacy in India: Concept & Evolution* 67 (Partridge Publication, New Delhi, 2016)

Mishra, Govind — *Right to privacy in India* 45 (Preeti Publishers, New Delhi, 1994)

Marath, Hariom — *Justice Delayed is Justice Denied* (Lexis Nexis, Butterworths, Nagpur, 2008)

Marcuse, Herbert — *Privacy And The Law : A Philosophical Prelude* 273 (Oxford University Press, London, 1966)

Gross, Hyman — *Privacy its legal protection*, 122 (Oxford University Press, London, 1976)

Pandey, J.N. — Constitutional Law of India (Central Book Publishing, New Delhi, 2017)

Rule, James B. — *Global Privacy Protection* (Edward Elgar University Press, America, 2008)

Dhar, Javed — *Privacy & Data Protection Laws in India*, 44 (Independently Published, New Delhi, 2018)

Salmond, John William — *The Law of Torts*, 44-46 (Arkosh Press, London, 15th edn., 2015)

Mathew, K.K. — Democracy, equality and Freedom 89 (Central Book Publishing, New Delhi, 1st edn., 1978)

Veshtak, Kiran — *Right To Privacy Under Indian Law* 76 (Deep And Deep Publications, New Delhi, 2012)

 ISSN: 2582-6433

Jain, M.P. *Constitutional Law* (Wadhwa & Company, Nagpur, 2007)

Baderin, Mashood A. *International Human Rights and Islamic Law* (Eastern Book Company, New Delhi, 2003)

Ramnath, N.S. *The Adhar effects : why world's Largest Identity Matters* 84 (Oxford University Press, New Delhi, 2018)

Kamath, Nandan *A Guide to Cyber Law* (Central Book Publishing, New Delhi, 2008)

Buba, Nicole M. *The Right to privacy & Data Protection laws* 98 (Princeton University, New York , 2005)

Diwan, Parag *Information Technology Laws relating to Cyber and E-Commerce* (Allahabad Book Agency, Allahabad, 2000)

Higgins, Paul O. *Cases and Materials on Civil liberties* (Sweet & Max well, London, 1980)

Kumar, Prof. Narendra *Constitutional law* (Allahabad Law Agency, Allahabad, 2008)

Wacks, Raymond *Personal Information Privacy and the Law* 20-21 (Oxford University Press, London, 1994)

Sharma, S. K. *Privacy Law : A Comparative Study*, 25 (Eastern Book Publishing, New Delhi, 1994)

Sathe, S.P. Right to Information 34 (Lexis Nexis, Butterworth's, New Delhi, 2005)

Joga Rao, S.V *Cyber Crime and Information Technology Law* (Universal Law Publishing, New Delhi, 2007)

Cooley, Thomas M. *Law of Torts* 91 (Oxford University Press, London, 1888)

Statutes :

- The American Patriot Act, 2001
- Justices of Peace Act, 1361 (34Edw 3 c 1)
- Indian Evidence Act, 1872 (Act 1 of 1872)
- The Registration Act, 1908 (Act 16 of 1908)
- The Constitution of India 1949
- The Telegraph Rules, 1951
- The Information Technology Act, 2000(Act 21 of 2000)
- Amendment of Information Technology Act, 2005

 ISSN: 2582-6433

- The Information Technology (Due Diligence observed by Intermediaries Guidelines)

Rules, 2011

- Indian Penal Code,1860(Act 45 of 1860)
- India Post Office Act,1898(Act 6 of 1898)
- Right to information Act,2005(Act 22 of 2005)

Reports :

- National Commission, 143rd Report On the Review of the Working of the Constitution on Fundamental Rights, Directive Principles & Fundamental Responsibility, (May, 2002)

Articles :

- Samuel D. Warren, "The Right to Privacy", 4 HLR 193 (1890)
- Justice R. S. Sarkaria, "Freedom of the Press: Defamation and Privacy", 15 PCIR 96 (1994)
- Govind Mishra "Privacy and the Indian Legal System", 12 DLR 63- 64 (1990)
- Hyman Gross, "Privacy its Legal Protection", 41 EPW 23 (1976)
- Nandan Kamath, "A Guide to Cyber Law" , 34 JILI 98 (2008)
- R.K. Suri, "Information Technology Laws law relating to cyber and E-Commerce", 87 JILI 89 (2000)

Website :

- http://www.epic.org.
- http://www.Jus,uio.no/iri/rettsinfo/lib/.html
- http://veda.wikidot.com
- http://ssm.com
- http://www.ndtv.com
- http://www.iamai.in
- http://indiankanoon.org
- http:/www.silicon.com
- http://www.mit.gov.inlitbillonline/itframe.asp
- http://www.aclu.org
- http://www.privacyrights.org

 ISSN: 2582-6433

- http://www.law.berkeley.edu/privacycensus.htm
- https://www.privacyrights.org
- https://www.startpage.com
- http://www.techtarget.com
- http://www.netscapeworld.Com
- www.rogerclarke.com
- http://www.oecd.org/documentl/html
- www.legalseviceindia.com

News Papers

- Hindustan Times