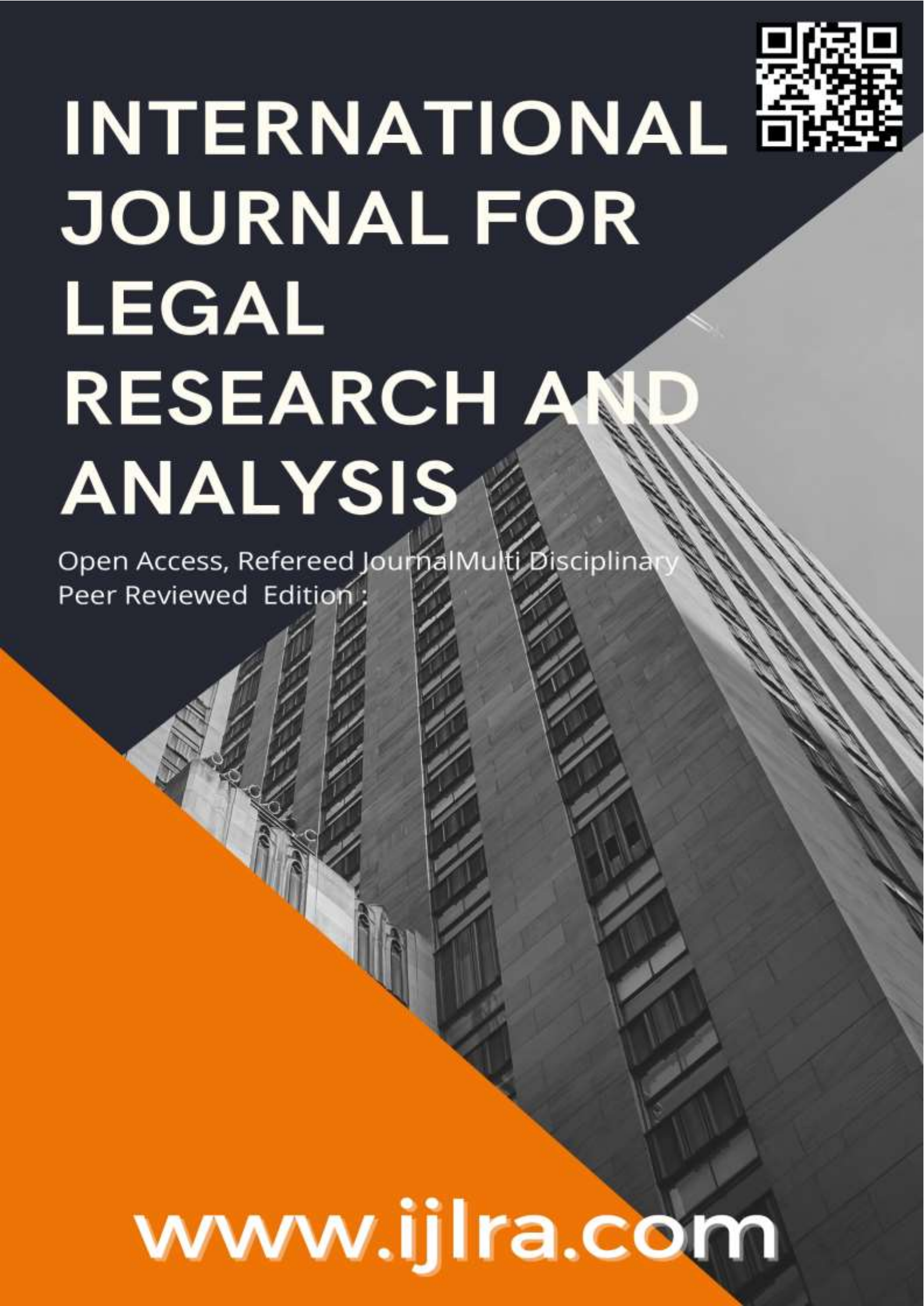
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

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 professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. 8Articles in various reputed Law Journals. Conducted 1Moot court competition participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Administration.10 paper presentations in various National and International Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Assistant Faculty, Published and

Justice seminars.

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

ESSENCE OF RIGHT TO PRIVACY UNDER ARTICLE 21

AUTHORED BY - KHUSHI BHATIA, A3221519243
AMITY LAW SCHOOL, NOIDA BATCH 2019 – 2024

DECLARATION

I, KHUSHI BHATIA student of BBALLB (H), hereby declare that the dissertation titled "Essence of Right to privacy under Article 21" which is submitted by me to Amity Law School, Noida in partial fulfillment of the requirement for the award of the degree of B.B.A.LL.B (H) by the Amity University, Noida is my original work.It is further declared that all the sources of information used in the dissertation have been duly acknowledged. I understand that the dissertation may be electronically checked for plagiarism by the use of plagiarism detection software to assess the originality of the submitted work.

NOIDA 22.04.2024
(SIGNATURE OF THE STUDENT)

(KHUSHI BHATIA)

CERTIFICATE

On the basis of declaration submitted by KHUSHI BHATIA student of BBALLB (H), I hereby certify that the dissertation titled " Essence of Right to privacy under Article 21" submitted to the Amity Law School, Noida in partial fulfillment of the requirement for the award of the degree of B.B.A.LL.B (H) by the Amity University, Noida has been carried out by her under my guidance and supervision.

(Signature) (Signature)

 ISSN: 2582-6433

ACKNOWLEDGEMENT

The completion of this dissertation owes much to the invaluable support and collaboration of numerous individuals. I want to express my heartfelt gratitude to those who have contributed to its realization. Foremost among them is my mentor and dissertation supervisor, Mr. Himanshu Varshney. His unwavering guidance, encouragement, and commitment to excellence have been instrumental throughout this journey. I have greatly benefited from his expertise, perspective, and passion for research. Our interactions have been enriching, fostering my ability to explore new avenues, challenge assumptions, and approach problems with analytical rigor and creativity. I am deeply thankful for his ongoing support, which has been indispensable in navigating the complexities of this endeavor. My appreciation also extends to my family and friends, whose steadfast encouragement has been a source of strength and motivation. Their unwavering belief in me has made all the difference.

TABLE OF CASES

 ISSN: 2582-6433

 ISSN: 2582-6433

List of Abbreviations

1.	AIR	All India Reporter
2.	ANR	Another
3.	APPL.	Appeal
4.	CRL.RC	Criminal Referred Case
5.	CPC	Civil Procedure Code
6.	CrPC	The Code of Criminal Procedure
7.	CIC	Chief Information Commissioner
8.	CS(OS)	Civil suit (Original side)
9.	DPAI	Data Protection Authority of India
10.	DNA	Deoxyribonucleic Acid
11.	ECHR	European convention on human rights
12.	EHRR	European human rights reports
13.	EU	European Union
14.	FIR	First information report
15.	HC	High Court
16.	HIV	Human immunodeficiency virus
17.	HST	Harmonized sales tax
18.	ICCPR	International covenant on civil and political rights
19.	IRDA	Insurance Regulatory and Development Authority
20.	ISA	Indian stamp act
21.	ISP	Internet service provider
22.	IT	Information Technology
23.	LTD	Limited
24.	ORS	Others
25.	PDPB	Personal Data Protection Bill
26.	PIPL	Personal Information Protection Law
27.	PLL	Petronet LNG Ltd
28.	RETD	Retired

 ISSN: 2582-6433

29.	RTI	Right to information
30.	SCC	Supreme court cases
31.	SC	Supreme court
32.	SCR	Supreme court reporter
33.	SEBI	Securities and exchange board of India
34.	SLP	Special leave petition
35.	TRAI	Telecom regulatory authority of India
36.	UN	United nations
37.	UDHR	Universal declaration for human rights
38.	UOI	Union of india

 ISSN: 2582-6433

CHAPTER -1 INTRODUCTION

1.1 Detailed Introduction

1.1.1 Definition of Privacy

According to Cambridge English dictionary privacy means:

"someone's right to keep their personal matters and relationships secret."

According to Collins English dictionary privacy means:

"If you have privacy, you are in a place or situation which allows you to do things without other people seeing you or disturbing you."

Privacy can have various meanings in different contexts but broadly privacy means when one person concedes or hide an information about themselves because it is sensitive to them, and they don't want others to know about it.

Privacy enables a person to create a shield around them to protect themselves from unwanted outside interference in their lives which allows them to portray the side which they want to show the world. For example, sexual orientation of a person is private, and that person have aright to keep it private. Every individual has a public life and a personal life and want to maintain a balance between both public and personal life. Human beings are not animals and have a certain way of living which varies from person to person as the society evolves the concept of privacy evolve.

Concept of privacy is as old as evolution of mankind, however nowadays its relevance has increased significantly. Although privacy became generally accepted in 19^{th} -20^{th} century, privacy had existed long before this timeline. Even Adam and eve covered their body with leaves in order to protect their privacy. In primitive societies there was very limited scope for self-determination (privacy) as most of their private life was influenced by the state. In the Medieval Era, there was no such thing as privacy as a social value in the modern sense; instead, people lived as members of a group, and their private lives were influenced by the continual "monitoring" by other members of society.

 ISSN: 2582-6433

1.1.2 Origins of Right to Privacy

In 1789, the United States Constitution went into effect. In the fact that the Constitution does not expressly grant the right to privacy, the Supreme Court has determined that the First, Third, Fourth, and Fifth amendments do.

In 1890 an article was published in Harvard law journal by Samuel Warren and Louis Brandeis[1] which was titled 'Right to Privacy' it became very famous among the legal scholars. They identified two factors that posed a danger to privacy: technology advancements and gossip, which had become a lucrative business in newspapers. In light of these considerations, they were the first to advocate for the recognition of a right to privacy, which ensured protection from not only land rights violations, but also emotional distress.

Members of the United Nations General Assembly drafted the Universal Declaration on Human Rights on December 10, 1948. Article 12 states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

India is no stranger to the notion of privacy. Meditation is prescribed by the ancient Indian system of knowledge, which is based on all Upanishad literature, and must be practiced without interruption. The houses, as well as the Arthashastra, show a great deal of thought and care for one's privacy.

Everyone wants to keep his private life to himself, while some think it's insane to do so. This private life enhances or detracts from, or in other words, molds, public life. An individual's interaction with the government was limited during the laissez-faire period. However, in today's administrative state, he must deal with the government in nearly every aspect of his existence. Information on individuals may be required by a government in order to formulate policies that are both intelligent and democratic. Surveillance by the government on its population is a key tool for social control. When it comes to providing social payments, the government may need to go deep into society and collect data. Personal information must be collected in order to prosecute today's organized criminals.

[1] Warren and Brandeis, "The Right to Privacy", Harvard Law Review193 (1890).

 ISSN: 2582-6433

Individuals working in departments related to the military, foreign affairs, and atomic energy may be subjected to government surveillance. While this process of information gathering may infringe on an individual's privacy, it is frequently necessary for the efficient functioning of government, particularly when the national interest is at stake. However, there should be an assurance that the governmental entity will only use such personal information for the objectives for which it was collected.

A right to privacy is recognized in both law and common use, although different legal systems place differing emphasis on different aspects of privacy, and privacy practices vary widely from culture to culture and context to circumstance. Many claims to the right to privacy are difficult to differentiate from other claims to personality rights, claims to respect for personal integrity, and claims against government and other external agents interfering with one's private life.

Privacy is a tough word to describe since it is exasperatingly imprecise and ephemeral, meaning various things to different individuals. This is because privacy is an emotive concept that encompasses a wide range of rights, some of which are interconnected and others that appear to be unconnected or contradictory. The capacity of an individual or a group to keep their lives and personal concerns out of the public eye, or to regulate the flow of information about oneself, has been defined as privacy. Judge Cooley gave the most basic definition of privacy: it is "the right to be left alone."

The advancement of technology, as well as the rise in the flow of information caused by computers, endangers an individual's capacity to manage the flow of information about himself—in other words, his privacy. The greatest pressing issue confronting mankind now is ‘information.' In reality, technological and scientific gadgets made it simpler to collect private or public data while also making it more difficult to govern how they were used.

Information about a person jeopardizes the privacy of his personal life, his family, and his residence. An unfair exploitation of one's personality or interference into one's personal conduct, known as invasion of privacy, is liable under tort law and, in some cases, constitutional law.

The Right to Privacy comprises a wide variety of subjects these are as follows:

- **Medical privacy**

Information about a person's health is kept private, and in most countries, the patient must give permission before it may be seen by anyone other than hospital staff. In other situations, however, failing to report

 ISSN: 2582-6433

one's medical condition may be unlawful. Medical privacy is being fiercely debated as a result of an increase in the number of medical breakthroughs such as brain mapping and DNA testing, which are unique to each individual.

- **Political Privacy**

  Although it may appear to be a contradiction, e-campaigning is the way of the future in today's society, with an ever-increasing number of internet users. It is easy to

[2] A.H. Robertson, Privacy and Human Right, London: Manchester University, Press, 1973, p.33

 ISSN: 2582-6433

obtain large amounts of information on which candidate a voter likes, whose websites he visits, and so on, using cookies, online contribution forms, and other methods.

- **Genetic Privacy**

  Genetic privacy is a term that has only lately entered our lexicon. It's required to avoid genetic discrimination based on visible or imagined genetic defects. Because of his family history of a certain genetic condition, a person may get dismissed from his work, lose friends, and so on, whether or not he is affected by it. As a result, genetic privacy is critical.

- **Internet Privacy**

  Unless you use privacy software or a proxy server, using the internet creates a trail of information about your usage. The history, cache, and logs of a web browser can be examined to see what the user did. Furthermore, the websites visited keep their own logs, which include the internet protocol addresses and other information for each machine to which they allow access.

  Other sorts of privacy include privacy during an online job hunt, privacy from companies, and privacy from government intrusion, among others.

1.1.3 Significance of Privacy as fundamental right in India

Privacy is something that practically everyone in the world values. It is our right to live our lives without the government intruding into our private lives. We may grow into individuals with our own views, opinions, goals, and goals thanks to privacy. It gives us the freedom to live our lives as we see fit in our own houses. Adults have the freedom to choose who they marry, whether they have children, and how they raise their families. The right to privacy limits the government's ability to look into our life.

Human rights are the fundamental protections that individuals must have against the state or other public authorities simply because they are members of the human family, regardless of other factors. Our lawmakers can give effect to any conservation in the shape of legislation for the good of society, according to Article 253 of the Indian Constitution. The development

 ISSN: 2582-6433

of the idea of personal liberty was aided greatly by human rights law. In several judgments, the Honourable Supreme Court acknowledged the right to privacy based on international convention.

It is past time for the government and the information technology industry to work together to find solutions to the problem of privacy invasion. Our legislators must defend privacy rather than pass laws that make it easier for individuals' privacy to be violated in the name of government activities.

The Right to Privacy is regarded a "penumbral right" under the Constitution, meaning it is a right that has been determined by the Supreme Court to be vital to the Fundamental Right to Life and Liberty[3], while not being directly mentioned in the Constitution. Furthermore, while no one legislation imposes a cross-cutting "horizontal" right to privacy, a number of legislation have provisions that either implicitly or expressly protect this right.

Even though the Indian Constitution does not expressly mention a right to privacy, the Supreme Court has read this right into the constitution as a component of two Fundamental Rights: Article 19 guarantees freedom, whereas Article 21 guarantees life and personal liberty. Before digging more into the privacy jurisprudence espoused by the courts under each of these Articles, it would be helpful to offer a little background to each of them.
Part III of the Indian Constitution (Articles 12–35) is titled "Fundamental Rights" and covers various rights that are considered fundamental to all Indian citizens. Article 13 of the Constitution prohibits the government from enacting “any law” that “takes away or abridges” fundamental rights.

Article 19(1) (a) states “All citizens shall have the right to freedom of speech and expression”. [4]However Article 19(2) stipulates that this will not “affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order,

[3] Article 21 of the Indian Constitution

[4] Article 19(1) (a) of the Indian Constitution

 ISSN: 2582-6433

decency or morality, or in relation to contempt of court, defamation or incitement to an offence".[5]
Thus, the right to freedom of expression provided by Article 19(1) (a) is a conditional right that can be reduced under certain situations within the Constitutional system. [6]

Article 21 of the Constitution is another key Fundamental Right in terms of privacy jurisprudence which states "21. No person shall be deprived of his life or personal liberty except according to procedure established by law."

In contrast to Article 19, which offers a specific list of criteria under which Freedom of Expression may be restricted, Article 21 is vague, requiring simply a "procedure established by law" as a pre-condition for the deprivation of life and liberty. However, in the well-known case Maneka Gandhi v. Union of India[7], the Supreme Court held that any procedure dealing with the modalities of regulating, restricting, or even rejecting a fundamental right falling under Article 21 must be fair, not foolish, and carefully designed to effectuate, not to subvert, the substantive right itself. As a result, "process" must rule out anything arbitrary or unusual.

1.1.4 Various Fields of operation of right to privacy

Right the to privacy is in various fields and express right is required when there is need for privacy.

Privacy in communications

All laws governing inter-personal communication media, such as the post, telegraph, telephone, and email, have similarly worded clauses allowing eavesdropping under certain instances.

The India Post Office Act 1898, for example, grants rights of interception of mail commodities for the "public benefit." This authority may be used "in the event of any public

[5] Article 19(2) of the Indian Constitution

[6] Despite of article 19(1) (a) of constitution of India there are reasonable restrictions imposed by state and these are (i) defamation; (ii) contempt of court; (iii) decency or morality; (iv) security of the State; (v) friendly relations with foreign states; (vi) incitement to an offence; (vii) public order; (viii) maintenance of the sovereignty and integrity of India. Thus, the right to privacy is limited against defamation, decency or morality. [7] (1978) 2 SCR 621

 ISSN: 2582-6433

emergency, or in the interest of public safety or tranquillity," according to this provision. The provision goes on to say that "a certificate from the State or Central Government" would be irrefutable proof of the existence of a public emergency or public safety or tranquillity concern.

Similarly, section 5(2) of the Telegraph Act allows for the interception of any transmission

a) in the event of a public emergency or in the public interest; and

b) if persuaded that doing so is necessary or expedient in the interests of India's sovereignty and integrity, state security, friendly relations with other states, public order, or preventing incitement to commit a crime,

The existence of any ‘public emergency' or in the interests of ‘public safety' are hence the events that warrant an interception action.

Thus, in the case of post and telecommunications, the terms "public emergency" and "public safety" give some legal buffer before the government may infringe on our private. They serve as both restrictions on our privacy and constraints on the government's power to infringe on our private, because the government must prove their existence to the court's satisfaction and if court is not satisfied their actions would be deemed illegal.

In addition to establishing procedural protections that limit the circumstances under which our communications may be intercepted, the law also protects our privacy by removing the evidential value of particular messages in specific circumstances. Conversations between spouses and communications with legal advisors, for example, are afforded a specific protection under the Evidence Act.

Married couples are prohibited under section 122 of the Evidence Act from exposing any communications made between them during their marriage without the approval of the person who made it. This does not apply, however, in cases involving “married persons” or “proceedings in which one married person is tried for a crime committed against the other.”

 ISSN: 2582-6433

Similarly, without their client's express agreement, section 126 of the Evidence Act prohibits "barristers, attorneys, pleaders, or vakils" from disclosing it simply states “any communication made to him in the course and for the purpose of his employment as such barrister, pleader, attorney or vakil... or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment or to disclose any advice given by him to his client in the course and for the purpose of such employment.”[8]

Section 127 of the Evidence Act extends the scope of attorney client privilege to include any interpreters, clerks and servants of attorney.

Clients cannot be forced to disclose confidential information between themselves and their professional legal advisors under section 129 of the Evidence Act.

Privacy in the home: search and seizure provisions

A residence or property may be inspected by a search warrant granted by a court or, in the absence of a court-issued warrant, by a police officer in the course of an investigation of an offence, according to the Code of Criminal Procedure (Cr.P.C). Police officers can conduct searches without obtaining a warrant under section 165 of the Code of Criminal Procedure. Such an officer must document the basis for his suspicions in writing and identify the object of the search "as far as practicable."

In all circumstances, the Code of Criminal Procedure mandates that the search be conducted in accordance with rules that include the presence of "two or more independent and respected local residents." The production of "a list of all objects seized in the course of such search, and of the places in which they are respectively located," in their presence, and the delivery of this list to the inhabitant of the premises being searched.

[8] Section 126 of Indian Evidence Act, 1872

 ISSN: 2582-6433

Privacy of the Body

This section examines the scope of one's right to privacy with one's own body in the context of four issues that have come before the courts: a) the state's ability to order people to undergo medical examinations, b) to submit to a variety of "truth technologies" such as narcoanalysis, brain mapping, and so on, c) to submit to DNA testing, and d) to abortion. As we will show, in most circumstances, the right to privacy gives way to any opposing interest.

Is it possible for courts to force people to undergo medical examinations against their will? The Supreme Court decided in Sharda v. Dharmpa[9] that they could. In this case, a man filed for divorce claiming that his wife had a mental disorder.

The court held that If the "respondent" avoids such medical examination on the grounds that it violates his or her right to privacy or, for that matter, his or her right to personal liberty as enshrined in Article 21 of the Indian Constitution, it may become impossible to reach a conclusion in the majority of such cases. It may render the fundamental reasons for divorce permissible null and void.

How much do pregnant women have a right to privacy when it comes to their bodies and reproductive choices?

The Medical Termination of Pregnancy Act, 1971 is amended on 25th march 2021.

- The opinion of one qualified medical practitioner will be required for terminations of pregnancy up to 20 weeks of gestation, and the opinion of two registered medical practitioners will be necessary for terminations of pregnancy between 20 and 24 weeks of gestation.
- Extending the upper gestation limit for particular groups of women from 20 to 24 weeks, including rape survivors, incest victims, and other vulnerable women (such as differently abled women, children), among others.

[9] (2003) 4 SCC 493

 ISSN: 2582-6433

- In situations of significant prenatal anomalies diagnosed by the Medical Board, the upper gestation restriction will not apply. The Medical Board's composition, functions, and other elements will be regulated later under the Act's Rules.

- The name and other personal information of a woman whose pregnancy has been terminated should not be disclosed to anyone unless allowed by law.

Do we have a right to privacy when it comes to the contents of our bodies, such as our blood, tissue, and DNA?

Genetic data privacy is a notion that tries to prevent a third party or someone else from utilising a person's genetic data without his consent. Science and technological advancements have made it simple to acquire DNA samples from people and extract personal information from those samples. However, these advancements are in violation of a person's right to private.

When a person's genetic data is utilised, whether for research, medical uses, or any other purpose, his privacy should be protected. De-identification is a crucial step in maintaining a person's privacy. A person's data is de-identified when he or she participates in a human experiment to preserve his or her privacy. De-identification is advantageous to health and research organisations because it allows them to use genetic information in study after certain identifiers such as a person's name and phone number have been erased. The data is always de-identified by genetic testing businesses. To protect anonymity, some businesses erase the identity from the data.

Genetic testing can provide information about a person's current and future health state. People who are more aware of their health will be able to make better decisions about their lives, diets, and treatments. They will be able to plan adequately for their therapy if they are aware of any sickness in advance.

Crimes such as rape and murder can be investigated, prosecuted, and detected using genetic information or genetic-based evidence. In addition to being utilised in criminal investigations, prosecutions, and detentions, it may also be utilised to clear someone of false allegations.

 ISSN: 2582-6433

The use of genetic data in criminal proceedings has the potential to bring justice while also safeguarding the public's interests. However, technology has posed a persistent danger to some of the most fundamental human rights, including as the right to privacy, physical integrity, and personal autonomy. We grant them access to our DNA by submitting it to a testing firm or a clinic. It reveals everything information about a person, whether physical or mental.

Genetic information is distinct from the other sorts of personal data. As a result, it requires special treatment. To preserve genetic privacy, new laws are being developed to govern direct-to-consumer testing. However, before joining up, the customer should read the company's privacy policy to avoid future problems. And, if the corporation violates its own policies, the proper law can be used to bring the firm to court.

The Delhi High Court found in Ms. X vs. Mr. Z & Anr [10]that an aborted baby was not a part of a woman's body and authorised a DNA test of the aborted baby at the request of the husband, notwithstanding the wife's objections based on her right to privacy. The woman's right to privacy is not violated by a DNA test on an aborted foetus.

The Delhi High Court was called upon in a high-profile case in 2010, Shri Rohit Shekharv. Shri Narayan Dutt Tiwari[11], to determine whether a man had the right to put the person he described as his biological father to a DNA test. The court used international treaties to uphold the "right of the kid to know of her (or his) biological antecedents" regardless of the legality of the child. The petitioner was able to present DNA evidence that ruled out the likelihood that his legal father was also his biological father in this instance. Furthermore, visual and anecdotal evidence pointed to the respondent as his biological father. The Delhi High Court directed the respondent to take a DNA test on these reasons. In an appeal to the Supreme Court, this was affirmed.

[10]AIR 2002 Delhi 217

[11] CS(OS) 700/2008

 ISSN: 2582-6433

The human body is prone to betrayal. We leave traces of our existence everywhere we go, from losing hair and fingernails to fingerprints and footprints, and handwriting, all of which may be implicated and identified against our will using modern technology.
Even our ideas are vulnerable, as emerging technology such as brain mapping claim to be able to extract psychic information from our physiology.

The court, according to Section 73 of the Evidence Act, "may require any individual present in the court to write any words or numbers for the purpose of allowing the court to compare the words or numbers so written with any words or numbers alleged to have been penned by such person."

The Supreme Court interpreted this provision in the case of State of U.P. v. Ram Babu Misra52, holding that there must be "any process before the court in which...it could be required... to compare such works."

The pre-independence Identification of Prisoners Act of 1920 requires police officers to take "measurements" and photographs of anyone arrested or convicted of a crime punishable by rigorous imprisonment for a period of one year or more, or who has been ordered to give security for his positive conduct under section 118 of the Code of Criminal Procedure.

The Orissa High Court upheld the constitutionality of ordering a DNA test in criminal proceedings to determine the participation of those accused in a case from 2004. If the accused refuses to cooperate, an unfavourable inference will be formed against him. After assessing the privacy issues, the court determined that the following factors must be considered before the DNA test can be ordered:

(i) “the extent to which the accused may have participated in the commission of the crime;
(ii) the gravity of the offence and the circumstances in which it is committed; (iii)age, physical and mental health of the accused to the extent they are known;
(iv) whether there is less intrusive and practical way of collecting evidence tending to confirm or disprove the involvement of the accused in the crime;
(v) the reasons, if any, for the accused for refusing consent”[12]

Both handwriting and finger imprints raise the question of whether they would violate our Constitution's guarantee against self-incrimination, which states that "No person accused of any offence should be

 ISSN: 2582-6433

compelled to be a witness against himself." In The State of Bombay v. Kathi Kalu Oghad and Others[13], the Supreme Court evaluated this point.

The court found that "compelling an accused individual to produce his specimen handwriting or signature, or imprints of his thumb, fingers, palm, or foot to the investigating officer or under court orders for the purposes of comparison" did not violate Article 20(3) of the Constitution.

The court distinguished between "statements" and "testimonies," concluding that only "statements" made under duress by an accused were forbidden under Article 20(3). It can only be referred to as the information acquired or extracted from the witness, according to the court.

In Selvi v. State of Karnataka[14], the Supreme Court recently invalidated this view. The Supreme Court, unlike the Bombay High Court, explicitly cited the right to privacy to declare these technology unlawful. The court went on to say that such approaches violated the accused's mental privacy, which was an important part of their personal liberty.

The court, on the other hand, left open the possibility of voluntary consent to such procedures and upheld the National Human Rights Commission's instructions. These requirements should be followed to the letter, and equivalent precautions should be used while doing the narcoanalysis methodology and the Brain Electrical Activation Profile test. The following is the text of these guidelines:

(i) "No Lie Detector Tests should be administered except on the basis of consent of the accused. An option should be given to the accused whether he wishes to avail such test.

[12] Thogorani Alias K. Damayanti vs v. State of Orissa And Ors, 2004 Cri L J 4003

[13] AIR 1961 SC 1808

[14] (2010) 7 SCC 263

 ISSN: 2582-6433

(ii) If the accused volunteers for a Lie Detector Test, he should be given access to a lawyer and the physical, emotional and legal implication of such a test should be explained to him by the police and his lawyer.

(iii) The consent should be recorded before a Judicial Magistrate.

(iv) During the hearing before the Magistrate, the person alleged to have agreed should be duly represented by a lawyer.

(v) At the hearing, the person in question should also be told in clear terms that the statement that is made shall not be a `confessional' statement to the Magistrate but will have the status of a statement made to the police.

(vi) The Magistrate shall consider all factors relating to the detention including the length of detention and the nature of the interrogation.

(vii) The actual recording of the Lie Detector Test shall be done by an independent agency (such as a hospital) and conducted in the presence of a lawyer.

(viii) A full medical and factual narration of the manner of the information received must be taken on record."[15]

Although the court's ruling was ultimately based on the right against self-incrimination and the intrinsic fallibility of the technologies, this case is noteworthy for the court's articulation of a right to "mental privacy" based on the basic rights to life and personal liberty.

[15] Ibid https://indiankanoon.org/doc/338008/ para223

 ISSN: 2582-6433

Privacy in records

From our birth and death records to our academic records, the majority of our essential transactions, our income tax filings, our food entitlements, and our citizenship, the majority of us have been chronicled and live a shadow existence somewhere on the files. Not only does the government store records about us, but so do a variety of commercial service providers such as banks, hospitals, insurance firms, and telecom firms keeps database of records. There can be breach of privacy via these records held with the government and the private sector.

Various legislation demand that records of operations carried out under their authority be kept, and whole bureaucracies exist exclusively to serve these papers. The Registration Act, for example, mandates the keeping of different registers that record papers that have been registered under the Act.[16]

These papers become public papers after they are registered under this Act, and State Rules normally include provisions allowing the public to access copies of all papers for a price.
Similarly, a number of pieces of law - usually dealing with state-level land records - have enabling clauses that allow the public to access them for a price or fee.

"The following documents are public documents :-
(1) documents forming the acts, or records of the acts –
(i) of the sovereign authority,
(ii) of official bodies and tribunals, and
(iii) of public officers, legislative, judicial and executive, 48[of any part of India or of the Commonwealth] or of a foreign country;

[16] Section 52 of the Registration Act 1908

 ISSN: 2582-6433

(2) Public records kept 49[in any State] of private documents."[17]

It is clear from above explanation that most documents available with government are public documents and section 76 of evidence acts states that every public officer who is having custody of a public document, which a person asked for to inspect, shall provide that person on demand a copy of it on payment of prescribed legal fees.

Only those with actual personal or financial interests in the subject may receive copies through this way.

In addition to the Evidence Act, citizens have the right to inspect and copy any information held by or under the control of any public authority under the Right to Information Act 2005, which grants citizens the right to inspect and copy any information held by or under the control of any public authority.

In a case where an applicant sought information from the Census Department on Sonia Gandhi's "religion and faith," the RTI adjudicatory apparatus upheld the denial of information on the grounds of privacy violation on several occasions, including in a case where an applicant sought information from the Census Department on Sonia Gandhi's "religion and faith." The rejection of information was supported by both the Central Information Commission, which adjudicates RTI cases, and the Punjab and Haryana High Court, as it would otherwise result in an undue intrusion into her privacy.

When private firms reveal personal information without a person's agreement, a similar idea of "public interest" appears to apply. Without going into too much depth on the subject, I'll just discuss one of the most important examples that has come up on the subject.

In Mr. X v. Hospital Z[18], a man sued a hospital when his HIV status was revealed to his girlfriend without his consent, causing their wedding to be cancelled. The Supreme Court ruled that the hospital did not violate patients' privacy because the information was disclosed to protect the public interest. While the court upheld the obligation of secrecy given to

[17] Section 74 Indian Evidence Act,1872

 ISSN: 2582-6433

[18] (2003) 1 SCC 500

 ISSN: 2582-6433

patients, it also said that the right to privacy is "subject to such action as may be legitimately taken for the prevention of crime or disorder, the preservation of health or morals, or the preservation of rights and freedoms of others."

In the case of *Subhash Chandra Agarwal v The Registrar, Supreme Court of India and Ors*[19], the question before the Hon'ble Delhi High Court was regarding the disclosure of information including details of medical facilities availed by individual judges. The Hon'ble Delhi High Court considered the fact that the total expenditure incurred for the medical treatment of the judges for the period in question was already furnished by the Central Public Information Officer and that it is not the case of the appellant that the said expenditure is excessive or exorbitant, and held that the "*details of medical facilities availed is personal information and there is no public interest warranting the disclosure of the same"*.

1.2 Statement of problem

Right to privacy is an important right but it is not an absolute right there are various gaps in implementation of right to privacy there are hindrances related to data protection, right to information procedures and constitutional loopholes. Spotting of the loopholes and gaps can be used in order to make suggestions for the betterment of the privacy laws in India.

1.3 Objectives of Research

- Analyse the present situation of privacy in India and how right to privacy play an important role in the life of individuals.
- Analyse how the right to privacy has evolved with the help of various judgements.
- To Analyse weather the existing provisions are sufficient.
- To analyse impact of privacy in various fields.
- To Address and analyse loopholes and gaps contributing to hindrance in effective implementation of privacy laws in India.
- To briefly analyse data protection and privacy laws in India.

 ISSN: 2582-6433

- To study the effectiveness of right to privacy laws.

[19] 2015 (150) DRJ 628

 ISSN: 2582-6433

1.4 Hypothesis

For the purpose of this dissertation, the researcher hypothesises that:

- The laws formulated for catering to protection of privacy of an individual are inadequate to deal with the surmounting crisis.

- There is not enough infrastructure, legal redress, and safeguard mechanisms for the victims of infringement of data vis-à-vis data privacy.

- The laws relating privacy protection have come along way but still they need to be more effective.

- There is lack of awareness and coherence amongst the duty holders entrusted with the task of ensuring compliance with the existing legislation relating to right to privacy in various aspects of law.
- There is immense delay in completing the entire trial and redress process which impedes with filing of cases or staying put throughout the entire judicial process of right to privacy.

- The domestic laws and policies of India are not at par with the developments around the world to stringently deal with cases of infringement of Right to privacy.

1.5 Research Questions

- What is the present status of right to privacy in India ?
- How the role of judiciary helped in evolution of right to privacy?
- What is the current situation of privacy laws in India with respect to constitutional restrictions, RTI procedures and data privacy?
- How hindrance in implementation of privacy laws affects the life of individuals?
- What is the impact of right to privacy on various fields and what effective measure does statues provide for privacy protection?

 ISSN: 2582-6433

- Whether the current manner of handling and disposal of cases relating to right to privacy serve the ultimate purpose behind the enactment of the law?

1.6 Research methodology:

In writing this dissertation, the researcher has adopted doctrinal and analytical method research to make a study of the existing rights and laws relating to right to privacy.

The researcher has extensive relied on the empirical data collected from secondary sources to gauge the on-ground working of privacy laws and implementing the existing laws and also to understand the challenges faced in implementing the existing privacy laws and further some recommendations for future.

1.7 Survey of Literature:

In order to comprehend and study the issue in hand as well as to meet the above mentioned objectives, the researcher referred to research in relevant field of study. Some of the most notable are listed below:

1.Warren and Brandeis, "The Right to Privacy", Harvard Law Review193 (1890).

This article explores the factors that posed a danger to privacy. In light of these considerations, Warren and Brandeis were the first to advocate for the recognition of a right to privacy, which ensured protection from not only land rights violations, but also emotional distress.

2. A.H. Robertson, Privacy and Human Right, London: Manchester University, Press, 1973 This report tries to provide a detailed definition of right to privacy and how it operates.

3.In 1921, Roscoe Pound, in his work titled “The Spirit of the Common Law”

This book explained the meaning of natural rights which says Natural rights are essentially interests that we believe should be protected; claims that humans may make which we think ought to be satisfied.

 ISSN: 2582-6433

4. In his Lectures on Jurisprudence (1869), Austin defined the public and private worlds and their distinction. He also says Every individual has a public life and a personal life and want to maintain a balance between both public and personal life. Human beings are not animals and have a certain way of living which varies from person to person as the society evolves the concept of privacy evolve.

5. John Stuart Mill essay, 'On Liberty' (1859) In this article, Mill expresses the necessity to retain a zone where citizens' liberty is unencumbered by governmental power. The acknowledgement of civil rights such as the individual right to privacy, free speech, assembly, and expression, according to Mill, might rein in the tyranny of the majority.

6. Legal service India e-journal on "Legal Analysis of Right To Privacy In India"

It shows the development of Right to privacy in India and the role of judiciary in achieving it.

7. Economic Law Practices-"Data Protection & Privacy Issues in India", September,2019 This article shows data protection laws in various fields and how various statutes provide provisions for data protection and also tells about the introduction of Protection of Data bill, 2018.

8. Article is based on "Why the Personal Data Protection Bill matters" which was published in The Hindu on 12/04/2021. It talks about how the personal data protection bill, 2019 can help in establishing a strong data protection regime.

1.8 Brief on the chapter

This chapter explains the definition of privacy, various dimensions in which it operate and its impact on various fields like privacy in communications, house, privacy of body, privacy of records and afterwards this chapter provides with statement of problem, hypothesis, research questions and methodology and finally the survey of literature.

 ISSN: 2582-6433

CHAPTER -2

JUDICIAL INTERPRETATION OF RIGHT OT PRIVACY THROUGH LANDMARK CASES

In primitive Indian societies, the idea of the privilege to protection could be followed out in the antiquated texts of the Hindus. Hitopadesh identifies those specific matters, for example, family matters, love and sex should be shielded from exposure. Security in old occasions was identified with 'positive profound quality'. However, this idea was unclear in the primitive Indian writings.

In modern India, the issue of the privilege to protection of Privacy was talked about for the absolute first time in the discussion of the Constituent Assembly, yet it was excluded from the Constitution of India. The issue of the privilege to security as an essential right under the Constitution and as a precedent-based law right has been managed since the 1960s.

Judiciary played a very important role in the development of right to privacy with passage of time the concept of privacy expanded and judicial approach towards it also changed.

2.1 Landmark Judgements that shaped the Right to Privacy in India

M.P. Sharma & Ors. vs. Satish Chandra and Ors.(1954) [20] this was the first time when Supreme Court come across and identified the privacy protection in India. An eight Judge Bench of the Court, while examining the lawfulness of the search and seizure provisons of the Code of Criminal Procedure, 1898 (CrPC), likewise momentarily talked about the right to privacy and its interaction with Article 20(3).

The Government of India requested an examination under the Companies Act, 1913 into the issues of an company after it went into liquidation in 1952. The examination was on the ground that the company had tried to steal funds and to cover the genuine situation from the investors, by misrepresenting asset reports and records. It affirmed that the exploitative and fake exchanges would comprise different offenses under the Indian Penal Code, 1860.

[20] (AIR 1954 SC 300)

 ISSN: 2582-6433

Likewise, a FIR was enlisted in 1953 and an application for a court order was submitted to the District Magistrate under Section 96 of the CrPC. The District Magistrate gave the warrant and synchronous search and seizures happened at 34 distinct premises. The Petitioner recorded an appeal in the Supreme Court requesting the court orders to be suppressed as being violative of Articles 19(1)(f) and Article 20(3) and mentioned for the arrival of the documents seized.

The Court dismissed the contention of the Petitioners that the option to acquire, hold and dispose the property was encroached upon by the search and seizure measure. The Court saw that the demonstration of directing the inquiry didn't deny an individual of the satisfaction in their property. Further, the Court noticed that however seizures included removing property from the influenced individual, it was just a transitory and restricted measure, and the State would be well inside its forces to hold onto things found during an inquiry. It was additionally noticed that seizures were just brief interruptions of the right to property and in this manner would not add up to an encroachment of the key right.

The Court at that point dug into the inquiry identifying with the right to protection against self-incrimination ensured under Article 20(3). It inspected the hypothetical contentions for and against the presence of self-incrimination and noticed that the presence of the right urges the police to complete dynamic examinations rather than exclusively depending on confessions. Given this foundation, the Court saw that the right ought not be barely perused and restricted to its literal meaning, and rather a liberal definition ought to be utilized which would propel the aim of the fundamental right. It noticed that Article 20(3) uses the term

"to be a witness" and not "to appear as a witness", and subsequently the protection against compelled declaration didn't just apply to oral declaration, however would include the compelled production of documents. Further, it was seen that under evidence law, one could be an witness by strategies other than giving oral evidence, through the production of documents. Accordingly, the Court held that Article 20(3) would apply to the production of documents just as oral declaration.

In any case, the Court couldn't help contradicting the Petitioner's conflict that search and seizure substituted summons, as it noticed that during the interaction of an inquiry and seizure, the warrant was routed to an government official, not the proprietor of the premises.

 ISSN: 2582-6433

In this manner, the accused had no role to carry out during the inquiry in delivering evidence. It was the activity of the public official which produced evidence, instead of the accused being constrained to give evidence. The Petitioners had contended that the search and seizure of reports added up to constrained creation which abused Article 20(3) and had relied upon the decision of the US Supreme Court in interpreting the Fourth Amendment of the US Constitution. The Court dismissed this contention as it saw that the Constitution of India didn't have a fundamental right to privacy practically equivalent to that of the Fourth Amendment of the US Constitution. The Court wouldn't import the standards of the Fourth Amendment as the right to privacy.

Kharak Singh vs State of Uttar Pradesh (1962)[21] in this case Kharak Singh, the petitioner, was charged with violent robbery in 1941 as part of an armed gang. He was released due to a lack of evidence, but under the Uttar Pradesh Police Regulations, a "history sheet" was opened under his name. For habitual offenders or individuals who are likely to become criminals, these regulations allowed for monitoring powers, including domiciliary visits.

The police would often patrol Singh's house at odd hours, waking him up while he was asleep, based on these provisions. The petitioner claimed that the regulations infringed on his right to a dignified life, which includes the right to privacy, as guaranteed by Article 21 of the Indian Constitution. He also stated that the steps infringed on personal liberty protected by Article 19 of the Indian Constitution.

The Supreme Court's six-judge bench reached a unanimous decision, declaring the related clauses of the Uttar Pradesh Police Regulations unconstitutional.

Justices Imam and Mudholkar, as well as Chief Justice Sinha, supported Justice Ayyangar's view. He pointed out that the legislation gave him many monitoring powers, including secret picketing of the building, domiciliary visits, and secret picketing of the house and investigating and shadowing so-called "history-sheeters" in order to keep track of their activities and contacts.

 ISSN: 2582-6433

[21] (AIR 1963 SC 1295)

 ISSN: 2582-6433

He dismissed the argument that the picketing's psychological impact limited freedom of movement under Article 19(1)(d), claiming that the concerned individual or visitors to the house will be unaware of the picketing.

Following that, he considered the issue of domiciliary visits. He said that this harmed the right to life guaranteed by Article 21 of the Constitution, which he described as the right to a life of integrity – not just animal nature. He believed that having the authority to access someone's home in the middle of the night to ascertain their existence was in violation of this privilege. This was clearly a violation of Article 21, since the right to life could only be limited by "rules," and the Uttar Pradesh Police's executive regulations did not meet the meaning.

Finally, he believed that shadowing the "history-sheeters" would not obstruct their campaign, and that any impact on privacy was unimportant because privacy was not a constitutional right. As a result, he argued that the rules could be overturned only in the case of domiciliary visits.

Justice Shah agreed with Justice Subba Rao's point of view. Insofar as the clause for domiciliary visits was illegal, they complied with the majority. However, Justice Subba Rao believed that the Regulations as a whole infringed on the right to freedom of movement and the right to life and hence not constitutional. The right to life and personal liberty under Article 21 offered immunity against any encroachment on personal liberties, whether direct or indirect, according to Justice Subba Rao. Even if the Constitution did not explicitly allow for it, he believed that the right to privacy should be considered a constitutional right under Article 21.
He went on to say that the regulations' supervision of one's private life obviously infringed on this privilege. Since the rules should not be considered "rules," they were found to be in violation of Article 21.

In addition, Justice Subba Rao believed that infringing on a person's right to privacy prohibited them from sharing their innermost feelings.As a result, he concluded that the legislation infringed on the right of freedom of speech guaranteed by Article 19(1)(a) of the Constitution. Furthermore, Justice Subba Rao found that the right to freedom of travel, guaranteed by Article 19(1)(d), has been violated, because this right encompassed not only

 ISSN: 2582-6433

freedom from physical impediments to movement but also the freedom to travel independently, without restriction.

He believed that police shadowing amounted to a restraint on his freedom of movement. As a result, Justice Subba Rao concluded that the rules as a whole violated human rights and were thus unconstitutional.

Govind v. State of M.P.(1975)[22] The Supreme Court confirmed that the right to privacy is a constitutional right in this situation. The right was said to cover personal intimacies of the household, marriage, family, and motherhood, among other things, but it was also subject to "compelling state subject."

In this case the petitioner is an Indian national. The legality of the Madhya Pradesh Police Regulations relating to monitoring, including domiciliary visits, was challenged by the petitioner. The petitioner claimed that false charges were made against him, and that he was placed under police surveillance as a result. The Madhya Pradesh police have identified the petitioner as a suspect based on his actions from 1960 to 1969.

The police began surveillance under section 46(2)(c) of the Police Act, 1961, articles 855 and 856. Because of his previous behaviour and history, the petitioner was on the police's radar. Many further cases is resolved in the future as a result of this decision.

Govind's appeal was rejected by the judge. Since they were established under Section 46(2)(c) of the Police Act, 1961, the court determined that Regulations 855 and 856 had the requisite legislative backing. The right to privacy does not exist unrestrictedly, according to the court. Article 21 contains some hints, but not any of them. Thus, fair limits on a person's Right to Privacy can be enforced, as decided by a thorough examination of the facts of the case and a compelling state interest hearing.

Police officers' domiciliary visits were not considered as breaching human rights because they were reasonable in intent and carried out with the aim of safeguarding the public interest. Domiciliary visits and monitoring are carried out on people accused of committing offences, so they are considered fair and legitimate.

[22] AIR 1975 SC 1378, (1975) 2 SCC 148

 ISSN: 2582-6433

The court instructed the police officers to exercise strict vigilance while acting in accordance with the regulations. To retain the importance of monitoring, only those in the clearest cases of illegal activity can be subjected to it.

R.Rajagopal v. Union of India (1994)[23] in this case a homicide prisoner (Auto Shankar) wrote a self-portrait.

The book looked at his relationships with a number of top prison officials, all of whom had been his accomplices in illegal activities. He was being held against his will at the time and may have been hanged. Prior to his death, he told his better half about his life by informing the jail authorities.

At that time, the spouse handed it over to the solicitors to distribute. The Examiner General of Prisons remained in contact with the dealers, arguing that the memoir series was fraudulent, that delivery was against jail rules, and that continuing to distribute would jeopardize lawful conduct. The book was meant to be disparaging in nature to the staff and prison professionals, but this was done for that purpose.

In this case court was of the opinion that any one has a right to privacy, and defaming others based on the conclusions of a single person whose views might be skewed is unethical and unconstitutional. As a result, even if elected authorities are doing a public service, they must have the same right of privacy in their official roles as anyone else.

It's also worth noting that everyone has the freedom to get his autobiography written because, according to Sec 19(1) of the Indian Constitution, everyone has a constitutional right to speech and expression.

Sec 19 (2) puts "fair limits on the freedom to free speech and expression," so any facts that cannot be verified as accurate should be published. Hence there was no proof that Gauri Shanker wrote the book therefore book should not have been published.

So according to the judgement Shankar was free to have his biography published in the case at hand because it was not written with malice aforethought and contained no misleading information. Only up to the point that no official secrets were violated was the information made public.

[23] 1995 AIR 264, 1994 SCC (6) 632

 ISSN: 2582-6433

In 2018, the concept of a right to privacy is a hot topic. However, it was not well-recognized in case laws and legislations in 1995. This case recognized the fact that privacy was not a constitutional right at the time. It was important for the development of this theory.

As a result, the Supreme Court addressed a discrepancy between press freedom and the right to privacy, concluding that the latter had gained constitutional status.

People's union for civil liberties v. Union of India (1996)[24] this case considered that telephone tapping is an infringement of one of a person's most valued possessions: privacy. The right to have a private telephonic conversation in the privacy of one's home or workplace, due to the expanded advancement of increasingly advanced technologies, is vulnerable to violence. The right to privacy of citizens must be safeguarded from government violence.

As a result, this writ petition was filed under Article 32 of the Constitution, alleging that the State abuses its authority over a citizen and that police officials repeatedly violate the Constitution's fundamental rights. The Petitioner adamantly argued that the right to privacy is a constitutional right protected by India's Constitution under Article 19(1) and Article 21. According to the Petitioner, in order to avoid Section 5(2) of the Act being ruled unconstitutional, the clause must be read down to include sufficient machinery to protect the right to privacy. The Court noted that the protection of one's privacy against unlawful police interference is fundamental to a free society, citing a precedent case on the principle of privacy and individual liberty as guaranteed under the Constitution.

The Court further laid down clearly that the right to privacy is a part of the right to “life” and “personal liberty” guaranteed under Article 21 of the Constitution. Article 21 is attracted in every situation concerning the right to privacy and this right cannot be curtailed “except according to the procedure established by law”.

The court stated in this case that the right to privacy is an integral part of the right to life and personal liberty, which includes the right to live with dignity.

The act of wiretapping is an infringement on each citizen's constitutional right to privacy, and thus constitutes a breach of the Constitution.

[24] AIR 1997 SC 568

 ISSN: 2582-6433

Distt. Registrar & Collector, Hyderabad & Anr vs. Canara Bank (2004)[25] in this case the Supreme Court debated parameters for fair search and seize practices in this case, ensuring that the universal right to privacy was not infringed upon. The Appellant, the District Registrar and Collector of Hyderabad, filed this appeal against an order of the High Court of Andhra Pradesh declaring Section 73 of the Indian Stamp Act, 1899, (the ISA), as amended by Andhra Pradesh Act No. 17 of 1986, is in violation of Article 14 of the Constitution and is incompatible with the state's other stamp rules.

The Court used Indian and American jurisprudence to map the origins and history of the right to privacy in deciding this case. It drew comparisons between the two countries, stating that people in both India and the United States have the right to privacy "both of the house and of the individual." The Court observed that even though a private customer's records were no longer at the individual's home but had been knowingly turned over to the Bank, the documents remained confidential. The Court further ruled that the State should not search or seize the records without any previous credible evidence justifying the inspection unless there was a probable or fair cause or justification.

As a result, the Supreme Court affirmed the High Court's decision that the revised Section 73 was unconstitutional and thus it mentioned "Once we have accepted in Govind and in latter cases that the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-a'-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank. If that be the correct view of the law, we cannot accept the line of Miller in which the Court proceeded on the basis that the right to privacy is referable to the right of 'property' theory. Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in the possession of the Bank tend, to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must necessarily be read into the provision relating to search and inspection and seizure so as to save it from any unconstitutionality."

The Court reached this decision after delving into the privacy interests of consumers in relation to their financial transactions. The Court reaffirmed the agreed Indian and American jurisprudence that the right to secrecy only applied to people, not locations, and declared that

25 (2005) 1 SCC 496, AIR 2005 SC 186

 ISSN: 2582-6433

"the customer's records or copies of documents in the Bank would continue to remain confidential even if the individual is no longer at the customer's residence and has willingly been sent to a bank." It referred to Seyman's case, which was settled in 1603 (77 Eng. Rep. 194) and established that 'Every man's house is his castle' and also Entick vs. Carrington ((1765) 19 HST 1029), which ruled that the protection to privacy covered trespass against goods, as well as the Fourth Amendment of the US Constitution, the Canadian Charter of Rights and Freedoms, and the New Zealand Bill of Rights, both of which contained clauses against "unreasonable search and seize."

The Indian Constitution, the Court observed, "does not contain a clear provision either as to 'privacy' or even as to 'unreasonable' search and seizure," but "the right to privacy has [...] been spelled out by our Supreme Court from the provisions of Article 19(1)(a) dealing with freedom of speech and expression, Article 19(1)(d) dealing with right to freedom of movement, and from Article 21, which deals with right to life, liberty, and property,"

The Court also cited the decision in Smt. Maneka Gandhi vs. Union of India & Anr., ((1978) 1 SCC 248), which stated that laws limiting rights under Article 21 "must meet a triple test:

(i) it must prescribe a procedure; (ii) the procedure must withstand the test of one or more of the constitutional rights conferred under Article 19 that may be available in a given situation; and (iii) It must therefore be testable in accordance with Article 14. Since Article 14's requirement also applies to Article 21, the law and practice approving interference with personal liberty and the right to privacy must be right, just, and equitable, rather than unreasonable, fanciful, or authoritarian. If the treatment recommended does not meet Article 14 requirements, it is not a procedure at all in the context of Article 21."

Petronet LNG Limited v. Indian Petro Group & Anr (2009)[26]The Delhi High Court was asked to determine whether the right to freedom of speech and expression was trumped by the right to secrecy and the circumstances of confidentiality.

Petronet LNG Ltd (PLL) is a publicly traded company with four public sector undertakings owning a combined 50% of the company and the general public owning 34.8 percent of the stock.

www.indianpetro.com (the "Website") is a website operated by Indian Petro Group ("IPG").

Petronet LNG Limited said in the current lawsuit that:

[26] Delhi HC – CS (OS) No. 1102/2006, judgment pronounced on April 13, 2009

 ISSN: 2582-6433

- Indian Petro Group violated the SEBI (Prohibition of Insider Trading) Regulations, 1992 (the "Regulations") by posting some papers on its website that exposed PLL's proprietary details of a price sensitive nature to the public.
- -Indian Petro Group also released inaccurate and deceptive facts about PLL's private dealings with third parties, weakening PLL's role in those negotiations and putting PLL in jeopardy of violating confidentiality clauses in numerous agreements it had signed.

The Hon'ble Court looked at a number of decisions, including Gobind Singh v. State of Madhya Pradesh, which dealt with the right to privacy. The right to privacy has been read into the "right to life" enshrined in Article 21 of the Indian Constitution in these decisions. The Hon'ble Court pointed out that in India, the right to privacy only extended to persons, and that no interpretation of the right could apply it to juristic or artificial bodies. Since there is no Indian case on the matter, the Hon'ble Court looked into the situation in Australia and the United States of America and discovered that the situations were close in both countries. Court observed non state actors don’t have fundamental rights.

The suit was maintainable under Section 9 of the Code of Civil Procedure, 1908 read with Sections 38 and 39 of the Specific Relief Act, 19634, because it was a suit to prevent the breach of a (implicit) obligation. After reviewing a number of English court decisions on the subject, the Hon'ble Court saw a change in the English courts' attitude toward the implied obligation for secrecy. The Hon'ble Court came to the opinion that there may be genuine questions regarding a corporation's or business's internal procedures, plans, and secrets in their early phases, which, if rendered public unnecessarily, may have permanent and unforeseen economic implications.

According to the court IPG was effective in generating public interest in news coverage and discussion of PLL's operations and the imposition of an injunction will jeopardise the basic nature of press freedom as well as the right of the general public to be told about the operations of an agency of which the Central Public Sector Undertakings own 50%.

As a result, the Hon'ble Court concluded that PLL must retain the Suit based on the assertion of its right to information secrecy. In a similar vein, the Hon'ble Court ruled that PLL's injunctions should not be issued. As a result, both the lawsuit and the provisional appeal is dropped.

 ISSN: 2582-6433

According to this judgement right to privacy is only available to individuals and not to companies and this right is only exercisable against state.

Selvi and others v. State of Karnataka and others (2010)[27] in this case Smt. Selvi and others filed the first round of criminal appeals in 2004, which were accompanied by appeals in 2005, 2006, 2007, and 2010, both of which were brought together by the Supreme Court via a Special Leave Petition on May 5, 2010. Objections have been presented in this new round of criminal appeals in cases where the victim, suspect, or witness in an indictment is an individual who has been sentenced to these proceedings without their permission. Such interventions have been defended, citing the value of extracting information that can assist enforcement authorities, deter potential illegal activities, even in cases where gathering evidence by traditional methods is difficult.

It has also been emphasized that using these procedures does no bodily injury, and that the information obtained will be used only for forensic purposes and will not be admitted as evidence during the research process. It is believed that better fact-finding during the inquiry process would result in a higher conviction rate and a higher percentage of acquittal.
Another point is that these scientific approaches are a viable solution to prosecutors supposed systematic use of alleged third-degree procedures. The primary issue in the case is the involuntary use of improvised tactics, which raises concerns about the defensive framework of Article 20 (3) of the Indian Constitution's right against self-defense.

The Appellant argued that these experimental approaches are a gentler solution to prosecutors' systematic use of third-degree procedures, and therefore a breach of Article20(3) constitutional right. The decision is unique in that it addresses both new facets of privacy and the right against self-incrimination guaranteed by Article 20 (3) of the Indian Constitution.

The bulk of the judgement was written by Hon'ble K.G. Balakrishnan (C.J.I.), who stated that Article 20 (3) of the Indian constitution places a strong focus on the issue of self- incrimination. However, in this entire ruling, the minority component of secrecy (right to

 ISSN: 2582-6433

[27] (2010) 7 SCC 263

 ISSN: 2582-6433

privacy) and due process has not been given an important position. It is, though, an essential and integral part of it.

During the last few years, the field of criminology has grown exponentially, and there has been a growth in demand for mutual approaches to boost the effectiveness of fraud identification and interrogation. Manual labor has been substituted for complex and time- consuming experiments in the proclamations of criminal operations in the assumption that straightforward approaches yield faster outcomes.

This decision concentrates on the most important aspect, namely the reading of Article 20(3). The minor part of the ruling, on the other hand, covers the basic elements of constitutionalism, including confidentiality and due process, which are less highly emphasized. While each part of the Constitution has its own features, a greater focus on minor problems of the verdict would help to balance the cause.

The early phase of the decision covered how any of these tests breaches privacy standards. However, when it insists on the 'Right of self-incrimination,' the weight of the decision seems to favor that side over privacy.

The Supreme Court ruled in this long-standing opinion that polygraph, brain-mapping, and narco-analysis are barbaric, inhumane, and humiliating treatments that are not lawful.

As a result, in the face of the growing number of violations against society, it is critical to consider the community's urgent needs, which necessitate a comprehensive and effective inquiry into human rights while ensuring that fundamental rights are not abused.

Unique identification authority of India & anr. v. Central Bureau of Investigation (2014)[28] in this case a Special Leave Petition was issued in response to the order of the Bombay High Court's division bench of R. S. Dalvi and F. M. Reis in Criminal Writ Petition No.10 of 2014. The writ filed in the Bombay High Court aimed to overturn a magistrate's order dated October 22, 2013, in which some data of people with Aadhar cards was given to the Central Bureau of Investigation (CBI) on the CBI's request under section 91 of Crpc,

[28] Petition(s) for Special Leave to Appeal (Crl) No(s).2524/2014 in the Supreme Court, Order dated March 24, 2014

 ISSN: 2582-6433

1973 (power to seek summons). The CBI had contacted the magistrate in connection with a rape case involving a seven-year-old girl that occurred in a school washroom and about which the CBI had been unable to find the perpetrator. The CBI, on the other hand, was able to recover certain fingerprints from the scene of the crime, which may aid in the identification of the perpetrator. The CBI requested information from the Unique Identification Authority of India ("UIDAI") in order to browse through the authority's database to see whether the fingerprints could be traced to someone in the database. The UIDAI declined to provide this material, claiming that it would infringe on the privacy of Aadhar card members.

The Supreme Court defined the conditions of fair searches and seizures in the case of District Registrar and Collector v. Canara Bank to ensure that a party's constitutional right against self-incrimination is not abused under Article 20 (3) of the Indian Constitution.

During the hearing, the UIDAI also told the High Court that several petitions relating to data kept by the UIDAI were pending before the Supreme Court, including Writ Petition No.
494/2012: Justice K. S. Puttaswamy v. Union of India. In the ad-interim order of September 23, 2013, a bench consisting of Justice Chauhan and Justice Bobde had held in the aforementioned writ petition about the fact that a government authority had released a circular making it mandatory to apply the Aadhar card to avail of such services, no one should suffer as a result of their lack of an Aadhar card. The UIDAI should ensure that Aadhar cards are not given to undocumented immigrants, according to the High Court. Following that, the Supreme Court issued subsequent directives requiring all states and unions to comply as they were made the parties. The Supreme Court is currently hearing this case in half.

The CBI had requested all available data in the state in the case before the Bombay High Court, but the appeal was later narrowed to three individual people. When the UIDAI declined to provide this detail, the CBI sent the UIDAI a CD comprising fingerprints it had collected and asked them to refer them to the biometric database. UIDAI believed that it lacked the necessary technology to parse through all of the biometric data it had in order to conduct the comparison. CBI responded by offering to evaluate UIDAI's database and conduct a comparison. The High Court stated that a comment on UIDAI's database's capability would be expected. It directed (on the Advocate General's recommendation) that the Director General of the Central Forensic and Scientific Laboratory select an expert, in

 ISSN: 2582-6433

addition to any other expert recommended by UIDAI, to determine the database's competence. Within two weeks, this submission must be lodged with the High Court. In current pleas on this topic pending before it, the High Court will consider issues of right to privacy and records, subject to the Supreme Court's order. The current SLP was filed in response to the contested order.

The Supreme Court, in an order dated March 24, 2014, stayed the Bombay High Court's preliminary order for the appointment of experts in Goa. Furthermore, the Supreme Court stated that an Aadhar card was not required to obtain any government service, and that any authority that made such a card obligatory would have to change its circulars and notifications to reflect this. Most notably, the Supreme Court barred the UIDAI from disclosing any biometric data in its servers without the permission of the data's holders in written format.

The Aadhar card was created to "issue per resident a unique identification number linked to the resident's demographic and biometric records, which they can use to identify themselves anywhere in India, and to access a host of benefits and services," according to the Central Government. Some governments, such as Delhi's, have made the Aadhar card a requirement for receiving the National Food Security Card, and a challenge to this is currently pending in the Delhi High Court. Furthermore, the government was beginning to make the card obligatory for LPG, rations, and other government services. The biometric is not an infallible norm, and there is a chance of mistake. As a result, using this information as an investigation method, particularly for appropriation by agencies like the CBI, is likely to have disastrous consequences. Furthermore, this will be a violation of Article 20 (3) of the Constitution, which protects individuals from self-incrimination. The object of submitting data to the UIDAI is solely for the purposes of Aadhar-related initiatives. When residents provided their biometric information, no permission was obtained from them that it could be used in possible investigations against them.

The National Identification Authority of India Bill, 2010, attempted to make the use of Aadhar data for national security purposes without the permission of the individual whose data was shared. However, the procedural viability of this bill, once it becomes law, would be checked against India's existing principles of self-incrimination law and privacy standards.

 ISSN: 2582-6433

In the case of, the Supreme Court ordered authorities to reverse any orders that made Aadhaar mandatory for receiving benefits. It also prohibits the UIDAI from exchanging any information in the Aadhaar database with any third party without the permission of the data subject.

Justice K.S. Puttaswamy & Anr. vs. Union of India & Ors (2015)[29]this case is the foundation of India's jurisprudence on the "Right to Privacy." In this situation, the nine-judge bench unanimously reaffirmed the right to privacy as a constitutional right under the Indian Constitution. The right to privacy, according to the Court, is an essential part of the liberties secured by human rights, as well as an inherent feature of equality, sovereignty, and liberty.

In light of the two rulings in the cases of M.P. Sharma vs. Satish Chandra[30], District Magistrate, Delhi, made by an eight-judge bench, and Kharak Singh vs. State of Uttar Pradesh[31], made by a six-judge bench, the Attorney General appearing for the State alleged that the validity of the right to privacy as a human right was in question. The State argued that both cases contained observations that the right to privacy was not expressly protected as a constitutional right under the Constitution. Simultaneously, numerous subsequent rulings have recognized the right to privacy as a constitutional right over the years. However, smaller benches than M.P. Sharma and Kharak Singh made the resulting decisions. Such confusions regarding right to privacy as a fundamental right resulted in a nine Judge Bench of Supreme Court in this case.

The case was started after Justice K.S. Puttaswamy, a former Karnataka High Court judge, filed a petition in relation to the Aadhaar Project, which was spearheaded by the Unique Identification Authority of India (UIDAI). The Aadhaar number was a 12-digit identification number provided to Indian citizens by the UIDAI. The Aadhaar project was related to a number of welfare programmes in order to streamline service delivery and exclude fake beneficiaries. Justice Puttaswamy filed a petition in which he questioned the procedural legitimacy of the Aadhaar card system. Other cases opposing various aspects of Aadhaar were appealed to the Supreme Court over time.

“The right to privacy is protected as an integral part of the right to life and personal liberty under Article 21 and as a part of the liberties secured by Part III of the Constitution,” the

[29] (2017) 10 SCC 1, AIR 2017 SC 4161

[30] (1954) SCR 1077

[31] (1964) 1 SCR 332

 ISSN: 2582-6433

Court unanimously concluded. It did so by overturning previous Supreme Court decisions in

M.P. Sharma and Kharak Singh, which held that the right to privacy was not recognised under the Constitution of India.

The Supreme Court declared privacy to be a constitutional right under Article 21 of the Constitution in six different opinions. This decision established a broad understanding of the right to privacy: it was not just a narrow right against physical violation or a derivative right under Article 21, but one that encompassed the body and mind, including decisions, choices, knowledge, and freedom. Part III of the Constitution was found to have an underlying, enforceable, and multifaceted right to privacy. The definition of the right was debated in detail in the various opinions. The Court upheld M.P. Sharma's decision, finding that the Indian Constitution did not include any exception to the rules on search and seizure similar to the Fourth Amendment of U.S. Constitution. The Court decided, however, that the Fourth Amendment was not an exhaustive concept of privacy, and that the lack of a similar guarantee in the Constitution did not mean that India lacked an absolute right to privacy – and therefore the M.P. Sharma decision was overturned.

The Court dismissed Kharak Singh's insular view of personal liberty ("ordered liberty"), which Justice D.Y. Chandrachud dubbed the "silos" approach after A.K. Gopalan. The Court stated that after Maneka Gandhi, this method to viewing fundamental rights in watertight compartments was abandoned. The Court went on to say that the majority opinion in Kharak Singh was internally inconsistent, since there was no legal precedent for striking down domiciliary visits and police monitoring on any grounds other than privacy – a right they mentioned in principle but found to be unconstitutional. The Court also held that subsequent rulings upholding the right to privacy after Kharak Singh should be read in light of the standards set out in the judgement.

The Court also considered whether the right to privacy was covered by the right to life, personal liberty, and the liberties provided by Part III of the Constitution in the affirmative case. It dismissed the Attorney General's contention that the right to privacy would be sacrificed in order for the state to have welfare benefits.

While noting that the right to privacy is not unconditional, the decision has included a summary of the judicial review standard that must be applied in situations of government interference into an individual's privacy. As previously said, the right to privacy is not

 ISSN: 2582-6433

unconditional. National protection would also be an apparent limitation, as would the provisos of various fundamental rights, depending on the context in which the right to privacy would be invoked. Another consideration will be the public interest.

Restrictions on the right to privacy can be justified under the following conditions, according to the proportionality principle:

a) Additional fundamental rights: The right to privacy must be weighed against other human rights and viewed in relation to its role in society.

b) Serious national security concerns

(c) Public interest, such as science or historical study or statistical purposes (see above)

(d) Criminal Offenses: the need for competent authorities to deter, investigate, and prosecute criminal offences, including protections against public security threats;

(e) Non-identifiable data: material that does not identify or identify a natural individual but remains anonymous. ‘pseudonymization' refers to the collection of personal data in such a way that it can no longer be linked to a single data topic without the inclusion of additional detail provided that if any additional information is stored separately and is subject to technological and organizational safeguards to prevent personal data from being linked to a known or recognizable natural person;

(f) Taxation and other matters: the tax regulatory system and the operations of financial institutions, as well as business conditions, may necessitate the disclosure of private information.

Simultaneously, Justice J. Chelameswar ruled that the "compelling state interest" requirement could only be applied to privacy arguments that need "strict scrutiny." He held that the just, equitable, and rational requirement under Article 21 will extend to other privacy claims. The enforcement of the "compelling state interest" principle, in his opinion, would be dependent on the nature of the case.

This case not only established the right to privacy as a constitutional right, but it also established the need for a new data privacy statute to be implemented, extended the definition of privacy in personal spaces, and addressed privacy as an inherent value. Informational

 ISSN: 2582-6433

secrecy was found to be a part of the right to privacy in the ruling. Although acknowledging the need for a data privacy regulation, the Court left it to Parliament to pass legislation on the matter.

2.2 Brief on the Chapter

This chapter provides a chronological data of landmarks judgements relating to right to privacy from M.P. Sharma & Ors. vs. Satish Chandra and Ors.(1954) to Justice K.S. Puttaswamy & Anr. vs. Union of India & Ors (2015) to show how the opinion of Indian judiciary have shifted and it have started recognizing the right to Privacy as a fundamental right under article 21 of constitution of India

 ISSN: 2582-6433

CHAPTER-3

INTERNATIONAL DIMENSIONS OF RIGHT TO PRIVACY

Writers around the Western world declare "privacy" as an incredibly necessary human good, a virtue that lies at the heart of what makes life worthwhile. Privacy is considered fundamental to personhood. In fact, the idea of what must be held "private," of what must be shielded from the gaze of another, seems to vary a lot from one culture to the next. This is an argument that is often made by quoting ethnographic literature, which shows us that there are certain cultures in which people happily defecate in front of others, and at least a few societies in which the same is true of having sex. However, invoking a vast historical literature that demonstrates how dramatically conceptions about privacy have changed and evolved over time may make the same argument.

3.1 International and Regional Human Rights Treaties

Many universal and regional human rights mechanisms include the right to privacy. The right to privacy for private or personal life, security of the home, and non-interference with communications is generally framed in broad terms. Data information access is not explicitly included as part of the right to privacy in any of the major human rights treaties. Even so, it is constantly being proposed that the ideals of data security are enshrined in these treaties' wider right to privacy.

- **The Universal Declaration 1948**

The Universal Declaration of Human Rights[32], adopted in 1948, is the foundation of all modern human rights instruments. The right to privacy is explicitly protected in Article 12 of the Declaration. It reads:
"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[33]

 ISSN: 2582-6433

[32] Universal Declaration of Human Rights, adopted and proclaimed by G.A. Res 217 A (III) of December 10,1948. UN Doc. A/810 (1948).

[33] Article 12 Universal Declaration of Human Rights

 ISSN: 2582-6433

The Universal Declaration of Human Rights is not a legally binding document. Rather, it is a resolution passed by the United Nations General Assembly to provide "a shared definition" of human rights and fundamental freedoms, as well as to provide "a common level of accomplishment" for these rights and freedoms. Despite its legal obscurity, the Declaration retains some legal meaning. It has evolved into a text of much greater legal power than regular General Assembly resolutions in the years since it was passed. In the very least, it is considered as the definitive interpretation of the UN Charter's term "human rights and fundamental freedoms," which member states are required to promote and obey.

- **The International Covenant on Civil and Political Rights 1966**

The controversy about the legal standing of Article 12 of the Declaration's right to privacy is primarily scholarly. Article 17 of the International Covenant on Civil and Political Rights contains an almost similar provision:

"1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks."[34]

The Covenant is a multilateral treaty that binds its members directly. The Covenant had 151 signatories as of December 2003, indicating that the right to privacy inherent therein has been almost universally accepted.

The Human Rights Committee, which was established by the Covenant to monitor its application and execution, released a general statement on Article 17's scope in 1988. Article 17 imposes a constructive duty on state parties to enact laws to protect persons from breaches of their privacy by both private and public entities, as well as a negative obligation on state parties not to comply with privacy "arbitrarily" or "unlawfully."

The committee's findings state that this right must be protected from all types of interference and threats, whether they come from government officials or private individuals. The duties imposed by this article compel the State to take statutory and other steps to put the ban on such interferences and attacks into effect, as well as to secure this right.

 ISSN: 2582-6433

34 Article 17 International Covenant on Civil and Political Rights 1966

 ISSN: 2582-6433

Furthermore, the Committee increased the provision's power and broadened its purpose by discriminating between "arbitrary" and "unlawful" interference. According to it, a "unlawful action" is one that is not permitted by law, and a "arbitrary intrusion" is one that is permitted by law but nevertheless contradicts the Convention.

The Committee specifically stated that the article's defense applies to individual's personal information. According to it states must take effective steps to ensure that knowledge about a person's private life does not fall into the possession of those who are not legally allowed to collect, handle, or use it, and that it is never used for reasons that are inconsistent with the Covenant. Any citizen should have the right to know, in an understandable manner, when and what personal data is contained in automated data files, and for what reasons, in order to have the most efficient security of his or her private life. Every citizen should therefore be able to determine which governmental officials, private persons, or bodies have power over or may have control over their personal information. Any citizen should have the right to request rectification or deletion of such files whether they contain inaccurate personal data or have been obtained or stored in violation of the law.

Unfortunately, no legally binding procedure exists for parties to enforce their Covenant rights. The Human Rights Committee is authorized by the Optional Protocol to the Covenant to collect and consider grievances from persons who appear to be victims of Covenant violations. However, the Committee's final rulings on the grounds of these complaints place no clear legal requirements on the state party in question, and there is no disciplinary process or penalty for noncompliance.

- **The European Convention on Human Rights 1950**

The Council of Europe ratified the European Convention on Human Rights in 1950, and it went into effect in 1953. The Convention is signed by all Council of Europe member states. The European Court of Human Rights is in charge of enforcing the Convention, and it has the authority to decide on citizen and inter-state cases claiming violations. Only the state parties to the lawsuit are bound by the Court's decisions. These rulings, however, have wider applicability to all member states because they are definitive representations of the Convention's rights and obligations.

 ISSN: 2582-6433

The right to protection for private and family life is guaranteed by Article 8 of the European Convention on Human Rights. It provides:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2.There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[35]

The article's framing in terms of a "right to respect" implies that states are not only obligated to refrain from interfering with an individual's private and personal life, residence, and communications, but also have a "positive duty" to pass legislation to secure these rights.

While the article does not expressly mention immunity from private parties, the European Court has indicated that such a duty can occur under such situations. In X and Y v.

Netherlands court observed that "these [positive] obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves."[36]

Article 8(2), like many other sections in the Convention, has a prohibition clause that outlines the types of interferences with the right to privacy that are allowable. Any intervention must be legal and "appropriate in a democratic society" in order to achieve one of the stated objectives. In terms of the Convention as a whole, it is well known that the mentioned restrictions to its provisions are absolute, and that no further prohibitions can be inferred.

Furthermore, the European Court has interpreted the requirement that limitations be "in compliance with the law" to mean that the regulation must be easily available, relatively precise, and not allow for the unrestricted exercise of discretion.

The Court has ruled that states have a "certain but not unlimited" margin of appreciation under the condition that limits be "necessary in a democratic society" in order to meet one of the enumerated objectives. If the Court does not demand that the measure taken be seen to be

35 Article 8 of European convention on Human Rights, 1950

36 March 26,1985, Series A, No. 91, para. 23.

 ISSN: 2582-6433

"indispensable," it does require that it led to a "pressing social need." In light of these stringent requirements, it is often argued that Article 8, along with its restrictions, offers greater security than the ICCPR's vaguely worded Article 17.

The Commission ruled in Chave nee Jullien v. France[37] that the storage of this material amounted to an infringement of the applicant's right to privacy under article 8(1), but that this infringement was justified under article 8(2).

The case of Z v. Finland[38] resulted from the seizure of the applicant's medical papers and their entry into the record during a court case against her husband for intentionally exposing others to the possibility of HIV infection. The domestic court required that her medical records be kept private for just ten years and that her name and HIV status be made public. This detail was then released to the public. As a result, the Court determined that the 10-year secrecy order and the refusal to preclude the declaration and release of the applicant's name and HIV status are an unjustifiable breach of her right to privacy.

In the case of MS v. Sweden[39], non-consensual sharing of patient information was also at issue. In this case, a hospital released the applicant's medical history to social security officials in order to determine her disability claim for a work-related accident. While the applicant's documents remained private, the court found that they had been revealed to "another public authority and thereby to a broader circle of public servants." In this case, however, it found that the intervention was justified under Article 8(2) because it was legal and proportionately served the legitimate goal of ensuring the country's economic well-being. It is unclear to what degree the constructive obligations of article 8 mandate states to shield people from data collection by private actors. The Human Rights Committee, on the other hand, has inferred a similar obligation from Article 17 of the International Covenant on Civil and Political Rights and the fact that member states of the Council of Europe accept that such practices must be governed by statute means that the European Court will read such a obligation into the article in question when it is presented before the court.

[37] (1991) Appl 14461/88,71 DR 141

 ISSN: 2582-6433

[38] [1997] ECHR 22009/93; (1998) 25 EHRR 371.

[39] Aug. 27,1997, Reports 1997-IV, 1437.

 ISSN: 2582-6433

- **The American Declaration of the Rights and Duties of Man, 1948**

Three clauses about privacy can be found in the American Declaration of Man's Rights and Duties. Articles V, IX, and X, respectively, contain the following provisions:

"a. Every person has the right to the protection of the law against abusive attacks on his honor, his reputation, and his private and family life;
b. Every person has the right to the inviolability of his home; and
c. Every person has the right to the inviolability and transmission of his correspondence."[40]

In May 1948, the recently formed Organization of American States adopted the American Declaration. The American Declaration, like the Universal Declaration of Human Rights, was not meant to have any legal impact at all, but its stature has changed with time.
The Inter-American Commission on Human Rights is in charge of fostering and ensuring that the Declaration's human rights are respected. It also developed a process for receiving and considering individual reports claiming violations of some of the Declaration's rights. The commission's rulings on the validity of these petitions aren't constitutionally binding on the applicants, and they can't be appealed to the Inter-American Court of Human Rights.

- **The American Convention on Human Rights 1969**

The American Convention on Human Rights adds to the Declaration's privacy guarantees. According to Article 11 of the Convention:
"1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks."[41]

 ISSN: 2582-6433

[40] Article 5,9 and 10 of American Declaration of rights and duties of man, 1948

[41] Article 11 of The American Convention on Human Rights 1969

 ISSN: 2582-6433

The Convention was ratified in November 1969 and came into effect in July 1978. The Convention had been ratified by twenty-four of the Organization's thirty-five founders as of December 2003. The Inter-American Commission on Human Rights and the Inter-American Court on Human Rights are in charge of monitoring and enforcing its provisions. Inter-state and citizen lawsuits claiming violations of the Convention can be sent to the Commission.

The Commission's conclusions and recommendations on these complaints are not constitutionally binding on the nations. The Commission, on the other hand, has the authority to refer cases of noncompliance to the Inter-American Court.

The Court has both advisory and adjudicative powers. Cases may only be referred to the Court by state parties and the Commission. Furthermore, an inter-state case can only be heard by the Court if both sides acknowledge the Court's jurisdiction.

3.2 The Right to Privacy in the United States of America

In the United States, the transformation of privacy and liberty issues into legally recognised rights is a comparatively recent phenomenon. The courts have created a revolution in autonomy privileges over the past few decades. The right to privacy gives residents of the United States a substantive right as well as a legal method to contest intrusive government regulations.

The United States' history shows that simply acknowledging the right to privacy is inadequate to explain essential autonomy interests. The privacy right's successful vindication by courts depends on procedural consistency and transparency in describing it. The experience of privacy legislation in the United States demonstrates that precedent can help solve the issue of inclusive rights at the expense of certainty. Tradition has the potential to easily delimit the boundaries of privacy rights without overly restricting them. A review of the American experience with privacy law would show that the British concern for procedural certainty should not have to be lost in order to better defend people's liberties.

Individual liberty is allegedly protected by the Constitution's expansive vocabulary, which ostensibly safeguards individual liberty from legislative encroachment. Around the same time, the Constitution incorporates a heavy injection of a democratic theory that means majority rule. In order to reconcile these conflicting constitutional norms, the Court has turned to community practice to support autonomy arguments. Despite the fact that the US privacy law is based on a different structural model from the British one, it suffers from the

 ISSN: 2582-6433

same flaw as the British regime: too much emphasis on majoritarian interests and little attention to the conflicting (majoritarian) principle of individual liberty.

In the United States, the federal judiciary, instead of Congress, is solely responsible for upholding privacy protections. While Congress has played a smaller role in the development of privacy rights than Parliament in the United Kingdom, it has passed several legislations that affect "privacy" concerns. In the 1960s and 1970s, technical advancements in data storage and processing significantly expanded the government's ability to infringe on human privacy rights. In addition, Congress passed legislation that established rights and responsibilities for the collection, storage, and distribution of personal information; however, these laws did not address individual autonomy. The federal judiciary was also in charge of upholding autonomy claims.

The Supreme Court started to establish a distinct privacy doctrine in the 1920s. Person preference was considered a valid object for judicial defense by the Court. Early precedents from the 1920s were used in the 1960s and 1970s to transform the right to privacy into a shibboleth capable of overriding state and federal legislation. In the 1980s, however, the Court re-examined the use to the right to privacy, as well as its precedents. In the United States, privacy law is at a fork in the track. In the end, the Court would have to choose between older decisions that stress human rights and recent decisions that emphasize the community's role in self-regulation by democratic institutions. While the right to privacy does not seem to be in imminent jeopardy, the current Court could seriously limit the right's reach. Current trends in privacy legislation in the United States show that recognizing a right to privacy did not fix all issues. It's possible that how a "right" is applied is almost as important as if the right is accepted at all.

Development of privacy Laws in United States of America

The formulation of US privacy legislation should have been mostly entrusted to state governments or the federal Congress. Instead, the federal judiciary has taken on the duty of preserving private rights from the directly elected majoritarian governmental branches, sheltered from the rigors of partisan politics. Invoking the Bill of Rights and the Fourteenth Amendment, the Supreme Court demanded that the government justify its conduct when challenged by persons who are aggrieved by state laws.

 ISSN: 2582-6433

In the 1920s, the Supreme Court invoked the fourteenth amendment's liberty clause to uphold citizens' right to privacy as a legitimate expectation. Meyer v. Nebraska[42] and Pierce v.
Society of Sisters[43] recognized that parents have a right to privacy in their children's upbringing. The Court acknowledged and confirmed a societal history of respect to parents in the training of their children, noting that the people of the United States thought that education and parenting of children was essentially the duty of parents. As a result, rather than assessing the customary method in which parents raise their children, the Court turned to the history of communal respect to parents parenting their children. The Supreme Court decided that an individual family's right to be left alone overcame the state legislature's finding that the parents were parenting their children inappropriately, drawing on the traditions of liberty instilled in American society through the Constitution.
Meyer and Pierce pioneered a concept that gained fresh traction in the 1960s. The Court considerably broadened the extent of the right to privacy, building on Meyer and Pierce's philosophical basis. To this aim, the Court defined privacy as a shadow generated by the Bill of Rights and the fourteenth amendment's plain textual requirements. Alternatively, several members of the Court viewed privacy as a specific type of liberty interest protected implicitly, if not expressly, by the ninth or fourteenth amendments.

The landmark decision of Griswold v. Connecticut[44], decided in 1965, marked a significant increase of the constitutional guarantee of privacy. The case highlighted the question of whether the state has the authority to regulate the personal aspects of a marriage. The case of Griswold involves a legal challenge to a Connecticut restriction on the use of contraceptive devices and the broadcast of contraceptive device instruction. Despite the fact that the Act had not been strictly enforced, it remained a barrier to effective family planning counselling and practice. Griswold, who is both a physician and the Executive Director of the Planned Parenthood League of Connecticut, counselled and instructed married couples on various methods of contraception. The Connecticut Act was overturned because it interfered too much with the marital bond, according to the Court.

Regardless of where the right to privacy originated, Griswold showed that people might assert privilege against some governmental rules. Meyer and Pierce's promise was realized in

[42] 262 U.S. 390,399-400 (1923)

[43] 268 U.S. 510, 534-35(1925)

[44] 381 U.S. 479,484-86 (1965)

 ISSN: 2582-6433

Griswold, with a full-fledged constitutional privacy concept. Although the right to privacy does not usually trump governmental rules, courts have begun to pay attention to arguments based on self-determination.

Despite the community's interest for its own security and well-being, the Constitution protects people against excessive government regulation of private life. However, the Court recognized that some liberty interests are too harmful to the community's survival to be tolerated.

In the abortion cases, the Court used Meyer and Pierce's stated criteria of communal respect to individual liberty. The Court, on the other hand, may be moving away from Meyer, Pierce, and Griswold. In contrast to Meyer and Pierce's heritage of liberty, the most recent privacy decisions show an alarming tendency toward the justification of majoritarian moral choices. The Court has used a novel and potentially harmful standard in instances involving sodomy and parental rights: the history of communal acceptability of a specific lifestyle. This new test incorporates majoritarian decision-making into what should be an examination of individual autonomy.

The controversial Roe v. Wade[45] decision, which gave women the right to abortion under the law, maintained the fundamental right to privacy established in Griswold. As a result, the Court's majority eventually agreed on a concrete articulation of a basic right to privacy.
Meyer and Pierce started the technique in the 1920s, and Roe finished it. Invasive governmental rules, according to the Court, could not impose an undue burden on legitimate autonomous interests. Roe's commitment to privacy has stood the test of time.

In Bowers v. Hardwick[46], the court decided that the right to privacy under the fourteenth amendment's liberty clause did not protect those who wanted to participate in private gay sodomy, despite the early trend of protecting individual choice in sexual and reproductive concerns. Before a private interest could be protected, the courts seem to require that the action in question be sanctioned by the community. Because "24 states and the District of Columbia" had laws forbidding sodomy, the Court concluded that such behavior could not be

[45] 410 U.S. 113,152-54(1973)

[46] 478 U.S. 186,190-91 (1986).

 ISSN: 2582-6433

considered "deeply established in our Nation's history and culture." This test implies that a person must demonstrate the community's approval of a certain behavior rather than the community's tolerance of individual choice in the area to justify a claim of privacy.

When courts uphold liberty interests, neither the community nor the court are obligated to approve a specific action. Rather, actions that recognize an individual's right to privacy simply indicate the community's readiness to let people make their own moral choices. Since the early privacy cases, both procedural and substantive consistency have been lacking in American privacy law. Tradition provides a reasonable way of limiting the extent of a right; procedural uniformity is a matter of judicial self-discipline. The right to privacy provides people of the United States with a level of liberty that is and is a function of both substance and process.

3.3 The Right to Privacy in the European Union

In general, most nations in continental Europe acknowledge a right to privacy or a right to one's own identity. The most prevalent type of trademark is one that protects a person's name and likeness. Other attributes, on the other hand, are frequently protected, even if they aren't directly stated in a legislation. These are conventional personal and private rights. Most governments provide them solely to protect citizens from invasions of their privacy, libel, and injured feelings. This is still a developing right, with no clear criteria regarding how it should be implemented or what it can encompass. Though the status of such rights differs by nation, there are certain general rules that apply to most European nations.

There is a requirement for nations that are members of the Council of Europe and have joined the European Convention for the Protection of Human Rights and Fundamental Freedoms[47], to defend certain rights and freedoms of their citizens. Article 8 of the Convention provides for a wide range of protections for an individual's right to privacy, stating that:

“1) Everyone has the right to respect for his private and family life, his home and his correspondence.

2) There shall be no interference by a public authority with the exercise of this right

[47] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4,1950.

 ISSN: 2582-6433

Hereafter called the ECHR.

 ISSN: 2582-6433

except such as in accordance with the law and is necessary in a democratic society and in the interests of national security, public safety and economic well-being of the
country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others."[48]

Article 13 of European convention for the protection of human Rights and Fundamental freedoms acts as an "right to an effective remedy" and it states:
"Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."[49]
If there is any uncertainty about whether a State has offered appropriate remedies to its citizens, an individual's complaint of a breach committed by his own nation can be heard by the European Court of Human Rights in Strasbourg. The Act's rights are not absolute, and they must occasionally be weighed against one another. This is frequently the case with Articles 8 and 10. The latter recognizes everyone's right to free expression and states that: "1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions, or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[50]

There is a set of regulations for member nations of the European Union that ensure a certain right to privacy for its inhabitants. The European Data Protection Act, often known as the European Data Protection Directive, established these laws in 1995. According to the Data Protection Act all member nations must establish legislation that protect the basic rights and

[48] ECHR Article8

[49] ECHR Article13

[50] ECHR Article10

 ISSN: 2582-6433

freedoms of natural people, in particular their right to privacy, with respect to the processing of personal data. The rule's goal is to prevent private information on people from being obtained and transferred without their permission "among commercial, governmental, or private information miners." “Any information related to an identified or identifiable natural person” is included in the personal data that can be safeguarded.

In some situations, the EU Data Protection Directive may apply if you have a claim based on the American concept of a right to privacy or publicity. A celebrity or private person may have a claim under the Act if his or her name, image, or other features are collected, processed, and utilized for commercial purposes via electronic transmission.

The aforementioned regulations are implemented and applied differently in different countries. The regulations given in European Acts, such as the ones stated above, are frequently excessive because the nations themselves have well-developed rules to defend the same interests. As a result, identifying a broad, homogeneous right in EU nations is challenging. It is necessary to examine the development in each nation in order to establish whether or not it would be able to unify rules in this area and what they would look like. It's also important to remember the varied ways that have been governing in each country to grasp what's going on in this field and where the countries are headed.

3.4 The Right to Privacy in the Great Britain

In English law, the right to privacy is not explicitly recognized. To the degree that privacy rights exist implicitly in the UK, they are expressed in a very different way than they are in the US. Indeed, in the United Kingdom, a popular book on privacy ignores freedom of choice in the domains of sexuality, reproduction, and familial/parental relationships. Although these problems are addressed under British legislation, they do not fall under the category of privacy. As a result, privacy rights in the United Kingdom are a "fragmented" issue.

There was no concept of privacy in early court rulings and laws. This reflects, in part, a reluctance to pass regulations governing any area of communal life. Furthermore, British governments oppose any legislative constraints on their ability to exert power. Britain has also refused to implement the European Convention on Human Rights' right to privacy on a national level. Despite the fact that Article 8 of the European Convention on Human Rights

 ISSN: 2582-6433

provides British residents the right to privacy, the United Kingdom is the only member to the convention without a privacy legislation. As a result, under domestic law, an individual citizen's ability to seek recourse against invasive government conduct is unguaranteed.

The notion of privacy has been grabbed by British people as a possible way of obtaining legal relief against overbearing majoritarian directives. Citizens have petitioned Parliament for the development of a legislative right to privacy, pushed for the enunciation of a common law right to privacy in domestic British courts, and requested the British judiciary to apply article 8 of the European convention on human rights and fundamental freedoms domestically.

Unfortunately, these attempts have mostly failed to establish an effective institutional structure to protect privacy rights. It's possible that an outside force will be required to compel legislative action. For example, the European Court of Justice might effectively compel the British government to acknowledge a right to privacy. However, in the absence of external pressure, reform prospects remain dim.

By legislation, Parliament has acknowledged numerous autonomous interests. To begin with, unlike many states in the United States, the British Sexual Offences Act permits homosexual sodomy in the house as long as it is not done for monetary gain. A second example is the British approach to the problem of prostitution. The British restrict solely public solicitation and pimping, rather than criminalizing payment for sexual; prostitution is not prohibited.

Abortion, on the other hand, is the finest example of when Parliament has intervened to protect an autonomous interest related with the right to privacy. In theory, the right to abortion in the United Kingdom is less protected than in the United States. Unlike in the United States, where a woman's "basic liberty" to choose whether or not to abort her fetus is protected by a "right of privacy," the British Abortion Act criminalizes abortion in the UK. In reality, however, the Act's exception provision swallows the entire, enabling legal abortions for the mother's or existing children's medical and mental well-being, as well as for deformed fetuses. The courts, with Parliament's implicit consent, have virtually enabled abortion on demand by generously construing this law.

The Data Protection Act of 1984, which governs the collecting and distribution of computer data, is a last example of statutory protection of restricted privacy concerns. An individual's right to access a computer database containing information about them is guaranteed under the Act. Parliament achieved this aim by mandating companies that gather personal

 ISSN: 2582-6433

information on computer databases to register and report on their activities. The Act, though extensive in its scope of applicability, has an exemption for the government when "national security" is at stake. The Data Protection Act, the Abortion Act, and the Sexual Offences Act are just a few instances of Parliament's readiness to safeguard privacy in certain circumstances.

Unlike the United States, British courts continually refuse to recognize or construct a right to privacy in any circumstance. "It is no function of the courts to legislate in a new field," British judges believe. Because the British courts consider law change to be a Parliamentary prerogative, it would be unusual for them to create a right to privacy on their own. Lord Simon, for example, refused to accept the tort of invasion of privacy in Director of Public Prosecutions v. Withers[51]. Despite the fact that the tort might potentially be drawn from the tort of breach of confidence, the Lord decided that taking legal action would be improper because Parliament was considering the subject. In the end, Parliament did nothing, and the subject of a common law right of privacy was still before the courts in the late 1970s.
Through judicial intervention, Article 8 of the ECHR provided a second avenue to a common law right of privacy. Article 8 was, however, rejected by the courts as a foundation for creating a common law right to privacy. Only where Parliament has expressly authorized or left some uncertainty in an authorization of invasive activity can the court protect privacy rights.

The inability of British domestic law to acknowledge a right to privacy does not rule out the possibility of such a right. Individual persons have a right to privacy under the European Convention on Human Rights (ECHR), which includes the United Kingdom. Because Parliament has declined to give the ECHR domestic effect, British courts do not uphold the ECHR's recognition of individual autonomy rights. If a society genuinely believes in liberty, it must advocate for liberty for all of its citizens. Different subgroups must have the opportunity to be heard inside the government's institutional structure. Furthermore, if the majority chooses to vest rights, it should ensure that claims to those rights are upheld regardless of the claimant's position.

[51] 1975 App. Cas. 842,862-63 (H.L.).

 ISSN: 2582-6433

3.5 Brief on the Chapter

This chapter shows that how right to privacy is a recognized right around the globe and its evolution. And how this right operates by way of and Regional Human Rights Treaties like UDHR 1948, ICCPR 1966, ECHR1950 and The American Convention on Human Rights 1969 and recognition of right to privacy in USA, European union and Great Britain.

 ISSN: 2582-6433

CHAPTER -4

DATA PROTECTION AND PRIVACY LAWS

4.1 The Concept of Data

The Information Technology Act of 2000 (the "IT Act") defines "data" under section 2(1)(o) as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer." According to the Digital Locker Authority 'data' means "any electronic information that is held by a public or private service provider (like a government service department, a bank, a document repository, etc. This may include both static documents and transactional documents'. However, the concept of data is not only restricted to electronic information but also extends to information stored in physical form, e.g. on a piece of paper".

Privacy of Data

The volume of data created by various electronic devices and apps has increased dramatically in recent years. Today's firms receive significant value from studying "big data," and they frequently build their business plans on it. While the corporate efficiency is undeniable, the burning question is whether or not individuals have control over how information about them is accessed and processed by others.

The right to privacy is the ability to be alone or to be free from the misuse or abuse of one's identity. The right to privacy is the right to be free from undue publicity, to live in isolation, and to be free from undue public intrusion in situations that are not necessarily of public importance.

The right to privacy is not a brand-new concept. It's a common law notion, and an invasion of privacy provides the victim the right to sue for tort damages. Semayne's Case (1604)[52] was one of the first cases on the subject. The case concerned the Sheriff of London's access into a

[52] Peter Semayne v Richard Gresham, 77 ER 194

 ISSN: 2582-6433

residence in order to carry out a legitimate writ. Sir Edward Coke famously observed, "The house of everyone belongs to him as his castle and fortress, as well for his defence against danger and violence, as for his relaxation," while recognising a man's right to solitude.

4.2 Issues in the Data Privacy

The Hon'ble Supreme Court in the case of K. S. Puttaswamy (Retd.) v Union of India[53], in which the ‘Aadhaar Card Scheme' was challenged on the grounds that collecting and compiling demographic and biometric data of the country's residents to be used for various purposes is a violation of the fundamental right to privacy enshrined in Article 21 of the Indian Constitution. Because of the uncertainty in earlier legal opinions on the constitutional validity of the right to privacy, the Supreme Court assigned the case to a constitutional bench of nine judges.

The Petitioners stated that the right to privacy is a fundamental right that is coterminous with the individual's liberty and dignity, and that this right is found in Articles 14, 19, 20, 21, and 25 of the Indian Constitution, as well as various international accords. The Union of India, on the other hand, argued that the ‘right to privacy' is not a fundamental right protected by the Constitution. The Supreme Court of India dismissed the Union of India's arguments, and while examining the essence of the right to privacy in terms of its origin[54], the right to privacy is essential to and inseparable from the human element in human beings, as well as the essence of human dignity, according to the Supreme Court[55]. As a result, it was determined that privacy had both positive and negative implications. The negative element prevents the state from infringing on a citizen's life and personal liberty, while the positive element requires the state to take all reasonable steps to preserve the individual's privacy.

As a result, under Article 21 of the Constitution, an invasion of privacy must now be justified by "a law" that specifies a fair, just, and reasonable approach.

 ISSN: 2582-6433

[53] (2015) 8 SCC 735.

[54] Ibid, para 53-65, 531-536, 718, 736.

[55] Ibid, Para 459.

 ISSN: 2582-6433

As a result, the "Adhaar Card Scheme," which was accused of infringing on the fundamental right to privacy, will now be held to the same criteria as a statute infringing on personal liberty under Article 21.

The Hon'ble Mr. Justice D.Y. Chandrachud concluded as follows when analysing the right to information privacy in today's world: -

"457. Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union government while designing a carefully structured regime for the protection of the data. Since the Union government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union government having due regard to what has been set out in this judgment.

746. We are in an information age. With the growth and development of technology, more information is now easily available. The information explosion has manifold advantages but also some disadvantages. The access to information, which an individual may not want to give, needs the protection of privacy.

747. The right to privacy is claimed qua the State and non-State actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the State."

The Supreme Court has established a three-part test for the state's interference with basic rights. While the State may intervene to protect legitimate state interests, (a) there must be a law in existence to justify an encroachment on privacy, which is an express requirement of Article 21 of the Constitution, (b) the nature and content of the law which imposes the restriction must fall within the zone of reasonableness mandated by Article 14, and (c) the

 ISSN: 2582-6433

means which are adopted by the legislature must be proportional to the object and needs sought to be fulfilled by the law[56]. As a result, any legislation that aim to impinge on an individual's right to privacy in the future must pass the proportionality and reasonableness test. The law will take several years to assess what constitutes fair and reasonable governmental engagement.

The Aadhar Scheme's legitimacy will now be questioned in light of this decision. It is frequently claimed that India should switch to a "rights-based" data protection paradigm rather than the current "consent-based" strategy. Once the user's approval is secured under the consent-based approach, the data controller is free to use, process, and share the data with any third parties. However, few people are aware of the true ramifications of inadvertent data sharing when they give their approval. The 'rights-based' model, on the other hand, allows users to have more control over their data while also requiring the data controller to guarantee that these rights are not violated. As a result, consumers have more control over their personal data.

The Honourable Supreme Court's ruling permits Indian people to seek legal remedies if their data privacy rights are violated. This might have ramifications for Indian IT businesses' privacy and protection practises. Users have the ability to bring claims based on torts as well as their basic right to privacy.

Nature of data that is protected by the Indian legislature

The IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 (the "IT Rules") are the key enactments that deal with data protection in India since the country lacks a comprehensive data protection structure. Under the IT Act and the IT Rules, what is primarily sought to be protected is 'personal information' and 'sensitive personal data or information', i.e. the information related to (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information. Information that is freely available in the public domain, on the other hand, is

[56] Ibid, para 447.

 ISSN: 2582-6433

not regarded to be "sensitive personal data or information." Furthermore, the regulations only apply to information collected and disseminated by a 'body corporate.'

In addition to the above, the respective sectoral regulators prescribe the data privacy measures required to be undertaken by (i) the telecommunications companies, (ii) the banking companies, (iii) the medical practitioners, and (iv) the insurance companies for protecting the privacy of data collected from the users and to avoid any unauthorised disclosures to third parties.

Who can collect the personal data?

IT Rules prescribes that "no body corporate or any person on its behalf shall collect sensitive personal data or information unless (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate; and (b) the collection of such information is considered necessary for that purpose."[57]

Further, "while collecting the information, the person sharing the information is required to be made aware of (i) the fact that the information is being collected; (ii) the purpose for which the information is being collected; (iii) the intended recipients of the information; (iv) the name and address of — (a) the agency that is collecting the information; and (b) the agency that will retain the information."[58]

Duration for which personal data can be stored

Anyone holding sensitive personal data or information on their behalf, whether a corporation or an individual, cannot keep it for longer than is necessary for the purposes for which the information may lawfully be used or is otherwise required by any law currently in force, and such information can only be used for the purpose for which it was collected.

Furthermore, before to collecting information, the body corporate or any person acting on its behalf must offer the supplier of the information with the option of not providing the data or information sought to be gathered. The information provider has the opportunity to withdraw its permission granted before at any moment whether using the services or otherwise.

 ISSN: 2582-6433

[57] Rule 5(2) of IT rules,2011

[58] Rule5(3) of IT rules,2011

 ISSN: 2582-6433

Extent up to which personal data can be shared with third parties

The body corporate receiving the information has the authority to disclose sensitive personal data or information to any third party if it has received prior permission from the information provider, or if such disclosure is agreed to in the contract between the recipient and the information provider, or if the disclosure is required to comply with a legal obligation. "However, no such consent from the information provider is required where the information is shared with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences."[59]

Obligations of the employers in relation to the personal data collected of its employees 'Sensitive personal information' of the employees is routinely collected by the employers such as financial information, health records, etc. If an employer stores such personal information on a computer resource, the employer, if a corporation, is required to have in place a comprehensive documented information security programme and policies that include managerial, technical, operational, and physical security control measures that are proportionate to the information assets being protected. Alternatively the employers can implement 'the international Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System – Requirements'.

Furthermore, under Rule 4 of the IT Rules, an employer who collects, receives, acquires, or maintains personal information about its workers must have in place a privacy policy for processing or dealing with such information. The employer must also make the privacy policy available to workers for review and post it on the company's website.

As may be seen from the foregoing, a comprehensive law governing the gathering and transmission of personal data is urgently needed. There are no comprehensive rules governing the processing of personal data that isn't considered to be "sensitive personal data or information."

[59] Rule 6(1) of IT rules,2011

 ISSN: 2582-6433

Personal data protection is intrinsically tied to privacy, which is defined as a person's right to enjoy his or her life and liberty without arbitrary interference in his or her private life, family, home, or communications. The term 'private' must be understood in contrast to the term 'public.' As a result, in today's intrusive Information technology era, the right to be left alone and its preservation are critical. Because there is no one law in India that rules data protection fully, the legal laws controlling it must be gathered from multiple legislative enactments. In this section, we looked at the essential statutory requirements that have an influence on how personal data is gathered and managed in India in detail. Furthermore, European data protection legislation have an extraterritorial reach, affecting data "controllers" and "processors" operating outside of the European Union ("EU") but dealing with EU data subjects.

Through the IT Act and the IT Rules, the government has established a legal framework for data protection and privacy. Following changes in 2008, the IT Act now includes a number of clauses relating to data protection, required privacy policies, and penalties for violating such policies. The following are the provisions of the IT Act that are relevant:

i) Section 43 (a), (b) and (i) - This section states that anybody who uses a computer, computer system, or computer network without the consent of the owner or another person in charge—

a) Gains access to, or obtains access to, the computer, computer system, or computer network in question;

b) downloads, copies, or extracts any data, computer data base, or information from such computer, computer system, or computer network, including data or information retained or stored on any removable storage medium;

c) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy, or alter any computer source code used for a computer resource with the intent to cause damage shall be liable for damages.

 ISSN: 2582-6433

ii) Section 43A - This section is the foundation of data protection and it states that a body corporate that has, deals with, or handles any sensitive personal data or information[60] in a computer resource that it owns, controls, or operates is liable to pay damages if it is negligent in implementing and maintaining reasonable security practises and procedures[61] and thus causes wrongful loss or gain to any person.

iii) Section 66 C – This section deals with identity theft and states that anybody who illegally or dishonestly uses another person's electronic signature, password, or any other unique identification characteristic is subject to imprisonment for up to three years and a fine of up to INR 1,00,000. (Rupees One Lakh)

iv) Section 66 E – This section states that anyone who intentionally or knowingly captures, publishes, or transmits an image of a person's private area without his or her consent, in a manner under circumstances violating the privacy[62], that person shall be punished by imprisonment for up to three years or a fine of not more than INR 200,000/- (Indian rupees Two Lakh), or both.

v) Section 72A - This section provides that, "any person, including an intermediary who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend up to three years, or with a fine which may extend up to INR 5,00,000 (Rupees Five Lakh), or with both."

The Information Technology (Amendment) Act of 2008 added four sets of rules.

- The Security Practices Rules impose strict security requirements on companies that retain sensitive personal information about users.

[60] Section 43A of Information technology Amendment Act,2008, Explanation(iii)

 ISSN: 2582-6433

[61]Ibid, Explanation(ii)

[62] Section 66E of Information technology Amendment Act,2008, Explanation(e)

 ISSN: 2582-6433

- The Guidelines for Intermediaries On the internet, there are rules that restrict some types of material. Such materials must be blocked by an intermediary, such as a website host.

- According to the Cyber Café Rules, cyber cafés must register with a registration agency and keep a log of users' identities and internet usage.

- The government can mandate that certain services, including as applications, certifications, and licences, be supplied online under the Electronic Service Delivery Rules.

The Cyber Cafe Rules may have negative consequences for users' privacy and personal safety

On April 11, 2011, the Department of Information Technology issued notice no. G.S.R. 313, which included the 2011 Rules for Information Technology (E). The following are the highlights of the 2011 Rules:

Only Indian corporations and individuals are covered by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. This was explained in a news release published by the Ministry of Communication and Information Technology on August 24, 2011, which said that the 2011 Rules applied to anybody corporate or individual residing in India.

The following are provisions in Information technology rules that are relevant to privacy:

- Information relating to passwords, credit/ debit card information, biometric information (such as DNA, fingerprints, voice patterns, etc. that are used for authentication purposes), physical, physiological, and mental health condition, and so on are all listed as “sensitive personal data” in Rule 3 of the 2011 Rules. Any information that is openly available or accessible in the public domain is not deemed sensitive personal data, according to the statement.

 ISSN: 2582-6433

- Body Corporates requesting sensitive personal data are required by Rule 4 to create a privacy policy and make it easily accessible to anyone giving the data. The privacy policy should be prominently posted on the body corporate's website and should include information on the type of information acquired, the purpose for which it was gathered, and the reasonable security methods used to protect the confidentiality of that information.

- Rule 6 of IT rules governs the body corporate's sharing of information to any third party. It states that a body corporate's sharing of sensitive personal data or information to a third party requires prior consent from the information's source. The third party receiving the sensitive personal data or information from body corporate cannot disclose it further. It is, nevertheless, mandatory to distribute the information to the government even without first getting the approval of the information source if such information includes sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The government agency must make a written request to the entity that has the sensitive personal data or information, explicitly describing the reason for the request. The government agency must additionally clarify that any information gathered in this manner will not be publicised or shared with anybody else.

Telecom Regulatory Authority of India

In India's telecom industry, there are a variety of applicable laws and policies that have requirements affecting the right to privacy and data security. These are some of them:

a) Sections 5 and 26 of the Indian Telegraph Act of 1885;

Section 5 of the Indian Telegraph Act of 1885 gives the government the authority to seize licenced telegraphs and order message interception in the event of a public emergency, or in the interest of public safety, or in the interests of India's sovereignty and integrity, the state's security, friendly relations with foreign states, or public order, or to prevent incitement to commit an offence. In such a case, the Central or State Governments, or any officer authorised by them, may, if satisfied that it is necessary or expedient to do so, direct that any class of messages to or from any person or persons, or relating to any particular subject,

 ISSN: 2582-6433

transmitted or received by any telegraph, be intercepted or disclosed to the government making the order, for reasons to be recorded in writing.

Section 26 states that if any telegraph officer, or any person with official duties connected with any office that is used as a telegraph office, wilfully, secrets, makes away with, or alters any message that he has received for transmission or delivery, or wilfully, and not in obedience to an order of the Central Government or of a State Government, or officer authorized by the government or omits to transmit, or wilfully intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or Any person who, without the permission of a competent court, divulges the contents, or any part of the contents, of any message to any person not entitled to receive it, or divulges the meaning of any telegraphic signal to any person not entitled to become acquainted with it, shall be punished by imprisonment for a term up to three years, or by fine, or by both.

 ISSN: 2582-6433

(b) Unified License condition 37, 39 and 42 of the Cellular Mobile Telephone Service license require the licensee, i.e., the telecommunications provider, to comply to particular confidentiality rules with regard to customer information in order to guarantee that communication privacy is protected and that unauthorised message interception is avoided. The licensee must not use mass encryption technology in its network, according to the agreement. Furthermore, the licensee must take all reasonable means to protect the privacy and confidentiality of any information about a third party and its company that it supplies or obtains as a result of the service supplied, and should use its best efforts to ensure that:

- No person operating on behalf of the licensee or the licensee discloses or uses any such information unless it is required to provide service to the third party;
- No such person seeks such information unless it is required to provide service to the third party.

The licensee must also take the appropriate efforts to ensure that customer information is kept secret by the licensee and anybody operating on its behalf, including its employees. The Telecom Regulatory Authority of India (TRAI) has issued a directive to all telecom and Internet service providers (ISPs) requiring them to adhere to the license's terms and conditions regarding confidentiality of information of subscribers and privacy of communications.

 ISSN: 2582-6433

4.3 Data protection in Healthcare

A. Mental Health Act, 1987 ("MH Act")

Section13 - This section allows an inspecting officer to visit mental hospitals, mental nursing homes, and visiting patients at any time, and the inspecting officer may demand the production of any records kept in accordance with the Mental Health Act.

Provided that "any personal records of a patient so inspected shall be kept confidential except wherein the inspecting officer is satisfied that any in-patient in a psychiatric hospital or psychiatric nursing home is not receiving proper treatment and care, he may report the matter to the licensing authority and thereupon the licensing authority may issue such direction as it may deem fit to the medical officer-in charge of the licensee of the psychiatric hospital, or, as the case may be, the psychiatric nursing home and every such medical officer-in-charge or licensee shall be bound to comply with such directions."

Section 38- According to this section visitors of mental patients are not allowed to see any personal documents of an in-patient that the medical officer-in-charge believes are confidential in nature.

B. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002

Regulation 7.14 –This regulation states that a registered medical practitioner shall not reveal a patient's secrets learned in the course of his or her profession except in a court of law on the presiding judge's orders; in circumstances where there is a serious and identified risk to a specific person and/or community; and in the case of notifiable diseases. In case of communicable / notifiable diseases, concerned public health authorities should be informed immediately.

 ISSN: 2582-6433

C. Health record privacy and harm to others.

4.4 The Aadhaar Act,2016 and Aadhaar (Aadhaar DS Regulations)(Sharing Regulations) Regulations 2016

The Government has recently mandated the use of the biometric database - Aadhaar to deliver targeted subsidies, benefits and services.

i. Section 28 – The authority must take all reasonable steps to ensure that the information in its possession or control, including information stored in the Central Identities Data Repository, is secure and protected against unauthorised access, use, or disclosure, as well as accidental or intentional destruction, loss, or damage.

ii. Section 29 – This clause makes it illegal to share core biometric information gathered or produced under the Aadhaar Act with anybody for any reason, or to use it for anything other than the production of Aadhaar numbers and authentication under the Act and, no identifying information shall be disclosed with a requesting entity except with the prior consent of the individual to whom such information belongs. Except for the purposes prescribed by rules, no Aadhaar number or basic biometric information must be published, exhibited, or uploaded publicly.

iii. Section 30 – This section specifies that biometric information will be considered sensitive personal information, and that the IT Act and its rules will apply to such

 ISSN: 2582-6433

[63] (2003) 1 SCC 500

 ISSN: 2582-6433

information in addition to, and to the extent not inconsistent with, the requirements of the Aadhaar Act.

iv. Section 37– This section outlines the penalties for exposing personal information, including imprisonment for up to three years, a fine of up to INR 10,000/- (Rupees Ten Thousand) or, in the case of a corporation, a fine of up to INR 1,00,000/- (Rupees One Lakh), or both.

v. Sharing Regulations 3 and 4 – These regulations provide that the authority's fundamental biometric information will not be shared with anybody for any purpose. Furthermore, the authority may share demographic information and an image of an individual with a requesting entity when the seeking entity obtains approval from the Aadhaar number holder.

vi. Sharing Regulation 5 –:This regulation states that anyone who collects an Aadhaar number must use it for a lawful purpose and notify the Aadhaar number holder of

 ISSN: 2582-6433

(a) the purpose for which the information is collected, (b)whether submission of an Aadhaar number for such purpose is mandatory or voluntary, and (c)alternatives to submission of an Aadhaar number, if any, and should receive the Aadhaar number holder's consent to the storage or use of his Aadhaar number for the purposes indicated. Such individual, agency, or business shall not use the Aadhaar number for any purpose other than those mentioned to the Aadhaar number holder while getting his consent, and shall not share the Aadhaar number with anybody without the Aadhaar number holder's approval.

4.5 Emergence of Protection of data bill, 2019

Now in recent times WhatsApp Inc. changed its privacy policy after being acquired by Facebook Inc., and users were notified that "WhatsApp" account information would be shared with "Facebook" to improve "Facebook" ads and product experiences, and users were asked to agree to the revised terms by September 25, 2016, to continue using WhatsApp. In light of this development, Karmanya Singh Sareen and others filed a writ petition in the Hon'ble High Court of Delhi, claiming that removing the privacy protection of"WhatsApp" users' data and sharing it with Facebook was a violation of the users' fundamental rights guaranteed under Article 21 of the Constitution.[64]

The Hon'ble Delhi High Court, in ruling on the case[65], stated that if users want to cancel their WhatsApp accounts entirely, WhatsApp must remove all of their data from its servers and avoid from sharing it with Facebook, In the case of users who want to stay in "WhatsApp," their current information/data/details will not be shared with "Facebook" or any of its group businesses prior to September 25, 2016.

[64] Karmanya Singh Sareen v UOI, 2016 SCC Online Del 5334.

 ISSN: 2582-6433

[65] Ibid.

[66] SLP (Civil) No. 804/2017

 ISSN: 2582-6433

Tushar Mehta, the Additional Solicitor General, filed an office memorandum with the Supreme Court on July 30, 2017. He briefed the Court about the formation of the Justice B.N. Srikrishna Committee, which would investigate data protection challenges in India, propose data governance principles, and create a data protection laws. In 2018, the Committee issued a report as well as a draft bill. The Personal Data Protection Bill, 2019 was tabled in the Lok Sabha by the government in 2019. It was also stated that it was based on a draft of the Justice
B.N. Srikrishna Committee.

WhatsApp released a new privacy policy in January 2021, giving users till February 28th, 2021 to approve and amend it. Some aspects of the revised privacy policy sparked criticism and appeared to be contentious: For example, the new policy does not provide users the opportunity to opt out of having their data shared with WhatsApp's parent firm, Facebook Inc. WhatsApp has extended the deadline for updating to 15 May 2021 in response to public outcry.

A writ petition was filed in the Delhi High Court shortly after the policy was revealed, challenging it. The new privacy policy, it said, infringed on the basic right to privacy by allowing WhatsApp to profile users' data without regulatory oversight. While this case is pending, the Confederation of All India Traders filed a similar petition at the Supreme Court. The Supreme Court refused to consider the writ petition since the case was already being heard by the Delhi High Court.

An application was filed in this case, Karmanya Singh Sareen v. Union of India, on February 15, 2021, opposing the new privacy policy. According to the app, WhatsApp offers less privacy protection in India than it does in Europe.

WhatsApp has refused to back down from its new privacy policy, which went into effect on May 15. The Indian government had already warned WhatsApp that company would face legal action if it did not reverse its unpopular policy. For the time being, Facebook's instant messaging app has struck a middle ground and stated that individuals who do not accept the new policy would not have their app's functioning limited.

 ISSN: 2582-6433

WhatsApp initially stated that it would delete the accounts of users not accepting the new privacy policy. After facing severe backlash, the company then made changes and said it would limit the functionality of the app. Following various developments, the Indian government asked WhatsApp to withdraw or revise the new privacy policy by March 25 and warned action against the firm stating it has "various options" available to it under Indian law.

The messaging service, which has over 400 million Indian users, has refused to do so until the Personal Data Protection (PDP) law takes effect.

The Srikrishna Committee prepared the PDP bill in 2018. The law was prepared in response to the Supreme Court's instruction to the Indian government to recognise privacy as a basic right. It is influenced by the EU's General Data Protection Regulation (GDPR).

The GDPR does not permit WhatsApp to share its data with Facebook or any other third party company. Similarly, when converted into a law, PDP would grant extensive data protection rights to Indian citizens while imposing limitations on the collection and processing of personal and sensitive data.

In WhatsApp's argument, the business is arguing that the PDP Law has yet to be introduced by the Indian government. WhatsApp will not make any modifications to its new privacy policy until the bill is passed. It will not, however, restrict WhatsApp's operation in the future weeks.

"We hope this approach reinforces the choice that all users have whether or not they want to interact with a business. We will maintain this approach until at least the forthcoming PDP law comes into effect," the statement said.

 ISSN: 2582-6433

4.6 Brief of the Chapter

This chapter tells about privacy of data and the relevance of data protection and also talks about various authorities and statutes that provides protection of data like Telecom Regulatory authority of India, information technology act 2000 and Indian Telegraph act 1855, Mental Health Act 1987 and Aadhar act,2016 this chapter shows the robust need for effective laws relating to data protection that the hon'ble supreme court pointed out after the Aadhar case[67] and talks about recent controversy of the WhatsApp case[68] and introduction of PDP bill that is prepared in 2018 but is yet to be implemented.

 ISSN: 2582-6433

[67] K.S. Puttaswamy v. Union of India (2015) 8 SCC 735

[68] Karmanya Singh Sareen v UOI, 2016 SCC Online Del 5334.

 ISSN: 2582-6433

CHAPTER -5 CONCLUSION

Article 21 of the Indian Constitution is a living provision that grows like an organism and inherits the energy necessary to meet the requirements of society. The ambition of the right to life and personal liberty continues to grow and will continue to do so in the future as a result of numerous court decisions and legislative enactments.

It acts as a tributary to all of the essential rights enumerated in Part III of the Indian Constitution. In light of recent occurrences in which our members of parliament debated an individual's privacy, it's important to remember that privacy is one of the most important aspects of personal liberty. As a result, it is a component of Article 21 and a right to be free of restrictions or encroachments on his person, whether enforced directly or indirectly. An illegal entry would constitute a violation of privacy, even though it is not addressed in the Constitution, Article 21, or any other Article of Part IV of the constitution.

According to a 9-judge constitution bench in the case (Justice K.S. Puttuswamy (Retd.) v. Union of India (2017) 10 SCC 1), the right to privacy is a basic right under Article 21.

The government and the information technology industry collaborate to find solutions to the problem of privacy invasion. Our legislators must defend privacy rather than pass laws that make it easier for individuals' privacy to be violated in the name of government operations.

Various legislative enactments in India do not confer protection of all types of data and loopholes exist in these enactments.

Loopholes in Information and Technology Act

- The IT Act only applies to the collecting and dissemination of information by a "body corporate."

- Under the IT Act, the phrase "consent" is not defined.

 ISSN: 2582-6433

- There is no definition of a data breach under the IT Act.

- The IT Act does not have an overarching provision stating that interception can only take place in circumstances of public emergency or public safety. Furthermore, under section 69 of the IT Act, any person or intermediary who fails to help the designated agency with the interception, monitoring, decryption, or provision of information stored in a computer resource is subject to a fine and a sentence of imprisonment of up to seven years.

- The IT Act's rules and procedures were designed to protect "personal information" an d "sensitive personal data or information" i.e. the information related to (i) password;
  (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition;
  (iv) sexual orientation; (v) medical records and history; and (vi) biometric information.
  However, material that is freely available in the public domain does not fall under the category of "sensitive personal data or information."

  Loopholes in Aadhar Act,2016

- According to Section 28 of the Act, the Authority is responsible for ensuring the security of people' identification information and authentication data. The Unique Identification Authority of India, created under sub-section (1) of Section11 of the Act, is referred to as a ‘authority' under Section2 (e) of the Act. It should be mentioned that Section 139AA of the Income Tax Act of 1961 allows Aadhaar to be linked to a PAN. The clause was challenged in the Supreme Court, but was upheld in the Binoy Viswam Case[69] by an Hon'ble Division Bench of Justices A.K. Sikri and Ashok Bhusan. When Aadhaar is linked, though, the UIDAI will share the data it collects with the Income Tax Authorities. However, the Income Tax Act makes no provision for any designation or authority to secure that information and data.

[69] Binoy Viswam v. Union of India and Ors (2017) 7 SCC 59

 ISSN: 2582-6433

- Because the Central Identities Data Repository (CIDR) is the centralised body for the storage and management of information, there is a huge risk of data breach or piracy, and if the centralised repository is hacked, millions of people's personal data and information might be exposed.

- It is a key notion that an individual's data must always be in his or her possession. However, it is important to highlight that the proviso to Section 28(5) of the Aadhaar Act prevents individuals from accessing the biometric data that is at the heart of their unique ID, therefore violating this basic principle.

- A court can only take cognizance of an offence punishable under the Act if UIDAI or any official or other person authorised by it files a complaint, according to Section
  47(1). Section 47 of the Act is arbitrary, unreasonable, and illogical since it does not give individuals a way to seek effective remedies when their right to privacy is violated. As a result, it is fair to conclude that section 47 infringes on people' rights to seek redress when their fundamental rights are violated.

- The UIDAI, which oversees the Aadhaar project, is also responsible for building a grievance redressal system[70] to resolve Aadhaar-related complaints, putting the grievance redressal body's independence in jeopardy.

 ISSN: 2582-6433

[70] Section 23(2)(s) of Aadhar act,2016

 ISSN: 2582-6433

- Section 29(4) is gives UIDAI broad discretionary authority to display, publish, or upload core biometric information of any individual for the purposes set out in the regulations.

Apart from the above mentioned loopholes there is Non-compliance with the Supreme Court's instructions under the Aadhar Amendment Act 2019.

- The Supreme Court in the Aadhar Judgement[71] held, " No doubt, the Government cannot take umbrage under the aforesaid provision to enlarge the scope of subsidies, services and benefits. 'Benefits' should be such which are in the nature of welfare schemes for which resources are to be drawn from the Consolidated Fund of India. Therefore actions by CBSE, NEET, JEE and UGC requirements for scholarship shall not be covered under Section 7 unless it is demonstrated that the expenditure is incurred from Consolidated Fund of India. We are of the opinion that the respondents shall not unreasonably expand the scope of 'subsidies, services and benefits' thereby widening the net of Aadhaar, where it is not permitted

- While maintaining Section 33, which dealt with mandatory disclosure in the interests of national security, the Supreme Court changed the decision-maker from Joint Secretary to a higher level in the Aadhar case and mentioned that " There has to be a higher ranking officer along with, preferably, a judicial

 ISSN: 2582-6433

[71] K.S. Puttaswamy v. Union of India (2015) 8 SCC 735 (para322)

 ISSN: 2582-6433

officer."[72] Despite the fact that a Secretary level official has been named in the 2019 Aadhar Amendment Act, no judicial officer has been included, therefore breaking the rule given down by the Supreme Court.

The actions taken by several nations imply that India needs to enact a robust Data Privacy Act to preserve citizens' information and defend their data privacy. Data Privacy Day was honoured on January 28th in the United States, Canada, Israel, and 47 European nations, although it has effects all around the world.

News regarding data privacy is circulating across the world, particularly in India, where a big number of users have begun migrating in significant numbers from a well-used messaging app (WhatsApp) to another (now well-known) app. While users in the EU are happy with the app despite the lack of a policy change, it has become a major source of concern for users in India. If we had a data protection regulation similar to GDPR, the fear would not have arisen. In India, there are currently no effective data protection laws in place. The Information Technology Act of 2000 (IT Act) is the sole law in place, and it provides grieved persons with a right to compensation for wrongful disclosure of personal information.

It's not as if such activities haven't been considered in the country. The Personal Data Protection Bill (PDPB), 2019, was introduced in the Lok Sabha by the Minister of Electronics and Information Technology, with the goal of protecting individuals' privacy in relation to their personal data and establishing a Data Protection Authority of India for such purposes and concerns. The law was unmistakably a positive step forward. The PDP Bill also wants to change the Right to Information (RTI) Act, which, according to critics, violates a "sound legal principle" that the right to information cannot be diluted by "abusing" the right to privacy. According to Section 8(1)(j) of the RTI Act personal information that has no connection to any public activity or interest may not be disclosed if it involves an unreasonable invasion of privacy unless one of the Act's public information agencies determines that the disclosure is in the public interest.

[72] (2015) 8 SCC 735 (para349)

 ISSN: 2582-6433

According to the PDP Bill, information on personal data that is likely to cause harm, when that damage exceeds the public interest, may not be shared. Who determines the likelihood of danger and whether it outweighs Public interest is unknown. It also removes the wording "which has no relationship to any public activity or interest" from the definition of personal information. For instance, the Chief Information Commission, which is outraged by the RTI's weakening73, claims that if an RTI is submitted to find out if a public worker was promoted despite disciplinary procedures, the information may be refused as "personal data." It has been stated that the RTI Act's privacy exception is already vulnerable to abuse, but further dilution would imply denial of fundamental rights and eroding democratic principles and constitutional liberties.

The following are some of the bill's most important features:

(a) Promote consent, purpose limitation, storage limitation, and data minimization, among other principles;

(b) Require agencies collecting personal data (data fiduciaries) to gather only the data necessary for a defined purpose and with the individual's express consent (data principal);

(c) Give individuals the right to receive personal data, correct erroneous data, delete data, update data, transfer data to other fiduciaries, and restrict or prevent personal data dissemination;

(d) Create an Data Protection Authority of India (DPAI) to safeguard individuals' interests, prevent abuse of personal data, enforce compliance, and raise awareness about data protection;

(e) Declare "social media intermediary" to be a significant data fiduciary whose acts have a major influence on electoral democracy, state security, public order, or India's sovereignty and integrity;

[73] TNN,"CIC slams draft personal data bill" Times Of India, Aug 22, 2018

 ISSN: 2582-6433

(f) Give individuals the "right of grievance" to file a complaint against a data fiduciary;

(g) Give the central government the authority to exclude any government agency from the proposed law's applicability;

(h) Provide for a "Adjudicating Officer" to decide penalties and award compensation for violations and a "Appellate Tribunal" to hear appeals against these;

(i) Empower DPAI to specify the "code of practise" to promote good data protection practises and facilitate compliance.

The bill, however, is currently waiting owing to a lack of information. Despite the fact that the bill provides a skeleton foundation for a data protection law and seeks to address some elements of data protection, it contains significant flaws:

- Courts of law and regulatory bodies should be authorised to define rules of fair and acceptable data processing, according to the Justice Srikrishna Committee's recommendations. The bill requires data fiduciaries to gather data in a fair and reasonable manner that protects an individual's privacy, but it does not clarify what constitutes a fair and reasonable means of Personal Data Processing.

- According to the bill the state has the authority to process data for the following objectives: I national security, (ii) law enforcement, (iii) judicial processes, (iv) personal or domestic reasons, and (v) research and journalism.

 ISSN: 2582-6433

As a result, it is clear that a legal exemption for national security may indeed be warranted. However, it is unclear whether exclusions for legal processes, research, or journalistic objectives fulfil the necessity and proportionality requirements.

- Only those government entities exercising functions directly related to the provision of welfare should be allowed non-consensual data processing[74], according to the Sri Krishna Committee's recommendations, and it acknowledges that non-consensual data processing by government entities for all types of public functions may be too broad to be considered an exception to consent.

- It's unclear why a simple breach of the principal's rights isn't enough to justify filing a complaint. The data principle must also demonstrate and establish that they have suffered harm as a result of unlawful data processing, putting an undue burden on the data principal. A complaint may be filed only in case of possibility of harm

- When it comes to data breach notifications, the law specifies that the data fiduciary must notify the Data Protection Authority For India (DPAI) "as quickly as possible" if the data breach poses a risk of "harm" to data principals.[75] This rule, however, is ambiguous because it does not specify how quickly or within what time frame the breach must be reported.

- The Data Protection Authority may direct the Recovery Officer to take a variety of enforcement steps against a person, including arrest, detention, property attachment, personal bank account attachment, and appointing a receiver to manage moveable and immovable property in exchange for compensation.[76] Unlike the Reserve Bank of India (RBI) or the Insurance

---

[74] S.13(2), Personal Data Protection Bill, 2018

[75] S.32(3), The Personal Data Protection Bill, 2018

[76] S.78, The Personal Data Protection Bill, 2018

 ISSN: 2582-6433

Regulatory and Development Authority (IRDA), the Bill gives the Recovery Officer unrestricted authority to act in accordance with the Data Protection Authority's instructions and does not require approval of a court order for the aforesaid enforcement activities.

As understood from various information sources, "there are only 12 non-EU countries that have data protection laws considered adequate by the EU (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US). Further, Australia, New Zealand, Hong Kong, and Japan have modelled their own data protection laws. Also, outside of its own country specific legislation, the US and the EU have adopted the EU-US Privacy Shield Framework. Not forgetting, while other countries are still in process of making their Privacy Laws, China published the first draft of its Personal Information Protection Law (PIPL) for public comment on 21 October 2020, which was their answer for GDPR, and too specific to rules in China."77

Different nations' actions show that India has to enact a robust Data Privacy Act to secure people' information and defend their data privacy, regardless of what happens in the Web world.

So far our country have come a long way from not even recognizing right to privacy to acknowledging it as a fundamental right and trying protecting it in every possible manner and in changing world most of public interactions are done online on various social media platforms and through internet mediums and other data fiduciaries. So while there are certain loopholes in the protection of data bill,2019 there are certain recommendations that can help improve it:

- Because the requirements of Section 4 of the Bill necessitate that data fiduciaries acquire data in a logical and fair manner, the PDPB shall only include regulations and recommendations for the fair and reasonable principles of data processing by data fiduciaries.

[77] Umesh Kumar, 'Why India is indifferent to the data privacy issue' Financial Express, February 13, 2021

 ISSN: 2582-6433

- The Data Protection Bill should allow the Data Protection Authority to issue consent forms for a variety of situations, and required organisations should follow these templates.

- To avoid misunderstanding, the inclusion of incidental objectives and the unclear phrasing of Section 5(2) of the Bill should be removed.

- The requirements of Section 13 are quite broad, and there is a risk that they will be arbitrarily applied under the umbrella of state duties. As a result, this provision needs to specify the realm of essential data in a more comprehensive and thorough manner.

- To ensure openness, data fiduciaries may be compelled to post information about any data breaches on their website.

- Instead of utilising a generic expression like as soon as feasible, Section 32 of the Personal Data Protection Bill should provide a clear time limit for the data fiduciary to disclose a data breach to the data processor.
- Despite the fact that the bill defines broad concepts, more effort is needed to make consent operate in practise.

- The addition of a qualified right to erasure in the Bill, as required by the GDPR, would have a substantial impact on people's privacy rights.

- In the event of a data breach, the Data Protection Authority might, in order to maintain openness, make the data protection impact estimates and data audits publicly available.

The PDPB has not yet been finalized. It is likely to be introduced during the next Parliamentary session. It is now a waiting game to see if it will become law in the following months. Let's wait and see how the final product turns out.

 ISSN: 2582-6433

BIBLIOGRAPHY

The researcher has utilized both primary and secondary sources in writing this dissertation.

The primary sources include international instruments; national legislation; and case laws in addition to the data collected in pursuance to be undertaken.

The secondary sources comprise several books, articles published in journals, magazines and newspapers, reports, and internet sources.

Internet Sources

1. http://www.legalservicesindia.com/article/2445/Evolution-of-Right-to-privacy-as-Fundamental-right.html
2. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/privacy-in- practice-2021-data-privacy-trends-forecasts-and-challenges
3. https://blog.ipleaders.in/know-the-right-to-privacy-in-india-its-sanctity-in-india/
4. https://privacy.sflc.in/universal/
5. https://www.un.org/en/about-us/universal-declaration-of-human-rights
6. https://www.thehindu.com/news/national/sc-verdict-on-right-to-privacy-what-each- judge-had-to-say-about-privacy/article19553856.ece
7. https://en.wikipedia.org/wiki/Privacy_laws_of_the_United_States
8. https://economictimes.indiatimes.com/news/economy/policy/view-whatsapp-case- is-about-you-the-average-internet-user-so-here-are-a-few-things-you-must-know/articleshow/83106416.cms?from=mdr

ISSN: 2582-6433

Articles, Books, journal, online journal, newspapers, report, etc.

1. Dorothy J Glancy, "The Invention of the Right to Privacy", Arizona Law Review (1979) Vol. 21
2. Warren and Brandeis, "The Right to Privacy", Harvard Law Review193 (1890).
3. "The Right to privacy in the Digital age", Report of the Office of the United Nations High Commissioner for Human Rights (30 June 2014).
4. "Report of the Group of Experts on Privacy", Government of India, (16 October, 2012)
5. Michael C. James, "A Comparative Analysis of the Right to Privacy in the United States and Europe," Connecticut Journal of International Law (Spring 2014), Vol. 29. Issue 2
6. A.H. Robertson, Privacy and Human Right, London: Manchester University, Press, 1973
7. Legal service India e-journal on "Legal Analysis of Right To Privacy In India"
8. Economic Law Practices-"Data Protection & Privacy Issues in India", September,2019
9. Article is based on "Why the Personal Data Protection Bill matters" which was published in The Hindu on 12/04/2021.
10. Umesh Kumar, 'Why India is indifferent to the data privacy issue' Financial Express, February 13, 2021