A Study on Judicial Trends in Privacy Law with Special Reference to Data Protection

SUMMARY OF THESIS

SUBMITTED TO THE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW

BABASAHEB
BHIMRAO
AMBEDKAR
UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

FOR AWARD OF THE DEGREE OF

Doctor of Philosophy

IN

LAW

SUPERVISOR
PROF. PRITI SAXENA
DEPARTMENT OF HUMAN RIGHTS

SUBMITTED BY
ARUN KUMAR MISHRA
ENROLLMENT NO.- 333/13

DEPARTMENT OF LAW
SCHOOL FOR LEGAL STUDIES
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
VIDYA VIHAR, RAEBARELI ROAD
LUCKNOW-226025

2020

SUMMARY

Introduction

The rapid growth of digital technology and proliferation of the internet have made it easier for anyone to collect, process, transmit and store information from anywhere in the world. The rapid development of technology over the last few decades has witnessed the emergence of several new legal and ethical issue. Unfortunately, the law has not kept up with the pace of technological development, leaving significant gaps in addressing many issues that arise from the use of these technologies.

It has always been said that technology is a doubled-edged sword. It brings enormous benefits in term of its efficiency and productivity; however, it also gives rise to concerns that the widespread use of technology may result in loss of privacy-specially data privacy. Technology such as surveillance cameras, mobile phone, satellite-based user location computation technology such as Global Position System (GPS) smart tags, bio-matric or radio-frequency identification (RFID) were not originally invented for invasion of privacy, but they have been used to achieve that purpose. Valuable information such as the personal data of individuals can now be collected, processed, and stored on a large scale at minimal costs. Individual are increasingly concerned about the harmful consequences that may arise from the misuse of their personal data.

Personal data can easily be accessed from a verity of sources. The government is also actively engaged in processing our personal data. Large volume of personal data is collected, stored, and processed by different governmental departments for a multitude of reasons and purposes from the moment we are born until we are dead. The processing of personal data has therefore become a key activity within the private and public sector.

As the importance of data privacy has garnered national and global attention over the past two decades, nations around the world have struggled to determine how to best regulate the protection of sensitive personal information. At the International

level, there are many important legal instruments dealing with data protection and Privacy Law were formulated, namely, the Council of Europe's Convention, and OECD Guidelines EU Data Protection Directive, APEC Privacy Framework, European Convention on Human Rights (ECHR), European Union Charter, Personal Data Protection Act (in various Countries). India has globally, as a party to the Universal Declaration of Human Rights (UDHR), and the International Covenant for Civil and Political Rights (ICCPR), acknowledged the right to privacy as a universal human right under Article 12 of the UDHR and Article 17 of the ICCPR.

At the National level there is no any proper law related to the Privacy and Data Protection. In India, issue of Data Protection is dealt in the "Information Technology Act, 2000". While Privacy issue deals with Article 21 Constitution of India.

In the Constitution of India, Law of privacy is recognition of the individual's right to be let alone and to have his personal space inviolate. The need for privacy and its recognition as a right is a modern phenomenon. It is the product of an increasingly individualistic society in which the focus has shifted from society to the individual. In early times, the law afforded protection only against physical interference with a person or his property. As civilization progressed, the personal, intellectual and spiritual facets of the human personality gained recognition and the scope of the law expanded to give protection to these needs.

Before the case of ***K. S. Puttaswamy and Others Vs. Union of India*** Right to privacy is not enumerated as a fundamental right in the Constitution. Under the constitutional law, the right to privacy is implicit in the fundamental right to life and liberty guaranteed by Article 21 of the Constitution. This has been interpreted to include the right to be let alone. The 'right to privacy' has been canvassed by litigants before the higher judiciary in India by including it within the fold of two fundamental rights: the right to freedom under Article 19 and the right to life and personal liberty under Article 21.

Recently in case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others*** a nine Judges bench decide that the "**The Right of Privacy is a fundamental right.** It is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make

autonomous life choices". Before the case of ***Justice K.S. Puttaswamy (Ret.) and Others Vs Union of India and Others*** supreme court of India in case of ***M P Sharma v Satish Chandra, District Magistrate, Delhi*** and ***Kharak Singh v State of Uttar Pradesh***, said that the right to privacy is not protected under the Indian constitution.

Statement of the Problem -

Present time, personal data is being collected and processed at a much larger scale that is not limited to AADHAAR, every application and website we use collects and processes our personal data. Our personal data is vulnerable to any non-State actor, private entity around the globe with the technological know-how to access and process this data unlawfully. Our personal data may be utilized by Non-State Actors to target Indian citizens through cyberattacks for financial gains as well as to profile the interests of any person.

Our personal data which is collect and process by the state and non-state sector, these state and non-state sector are falsely claim that it is voluntary, requiring to share personal data like biometric information and other information even if you do not wish to share anyone, which creates privacy issues of the individuals in relation to which people are unaware it is a great problem.

On the other hand, there is a big problem before judiciary to dispose-off privacy matter's which is related to data protection. Because there is no specific legislation related to data protection. Judiciary dispose of the data privacy matters through the Constitution of India, 1949, Information Technology Act, 2000, SPDI Rule, Aadhaar Act 2016, Credit Information Companies (Regulations) Act 2005, Indian Telegraph Act, 1885, Telecom Regulatory Authority of India act, 1997, etc. These Acts are not sufficient for the judiciary to dispose off the data privacy matters. So, its require to frame a specific legislation related to the data protection for present and future generation. So, it becomes necessary to work on these issues elaborately.

Hypotheses -

For the purpose of this study, the following hypotheses are formed:

1. Prospective of Data of Individual's Privacy.
2. Disclosure of Personal Data to Intelligence / Law Enforcement Agencies
3. Authenticity and Security of Personal Information and Issues with Sharing Information Collected by the Government and Private Agencies
4. Time Period for Maintaining Authentication Records.
5. Data of Individual and others Entities Protected by Judiciary.

Research Methodology -

The research work in the present study will be doctrinal and analytical research. For this literature from primary and secondary sources like various Acts & Statutes, Law Commission/Committee Reports, Judgements of Supreme Court and different High Courts, Lok Sabha & Rajya Sabha Debates, books written by various authors and articles found in journals, Legal Periodicals, Magazines will be collected. Further comparative, analytical, descriptive and evaluative methods to study and analysis the provisions of Data Protection Laws with under developed and developed countries relating to Data Privacy will be studied in a non-doctrinal method.

Objective of the study -

In view of the above, the researcher, during his research work, through the extensive study, desires to achieve the following objectives.

- To make a comparative study of Indian legal and institutional framework available for Privacy and Data Protection and in developed countries.
- To study and resolve the issue of privacy with Special reference to Data protection

- To analyse the legal issues and challenges which is hurdle in Privacy vis-a-vis Data Protection
- To assess the future strategies and to suggest measures and mechanism for implementation of privacy laws based on the findings of the study.

Tentative Plan of the Study -

The study will be divided into seven chapters under the following headings:

Chapter I- Introduction

Chapter II- Right to Privacy and Data Protection

(a) International Perspectives
(b) National Perspectives

Chapter III- Impact of Social Media on Data Privacy

Chapter IV- Comparative Analysis of "The Data (Privacy and Protection) Bill, 2017" and "The Personal Data Protection Bill,2018"

Chapter V- Judicial Travelling on the Issue of Privacy and Data Protection

Chapter VI- Findings of Non-Doctrinal Case Method.

Chapter VII- Concluding Remarks

(a) Conclusion
(b) Suggestions

Chapter II A-Right to Privacy and Data Protection: International Perspective

In this chapter I discussed that the international provision related to the data protection. I discussed the many important legal instruments dealing with data protection and Privacy Law were formulated, namely, the Council of Europe's Convention, and OECD Guidelines EU Data Protection Directive, APEC Privacy Framework, European Convention on Human Rights (ECHR), European Union Charter, Personal Data Protection Act (in various Countries). Universal Declaration of Human Rights (UDHR), and the International Covenant for Civil and Political Rights (ICCPR), acknowledged the right to privacy as a universal human right under Article 12 of the UDHR and Article 17 of the ICCPR.

Chapter-II B Right to Privacy and Data Protection: National Perspectives

In this chapter I discussed law related to Data Privacy protection in National Prospective. At the National level there is no any proper law related to the Privacy and Data Protection. There is no specific legislation related to data protection. At the national level the data privacy matters resolve through the Constitution of India, 1949, Information Technology Act, 2000, SPDI Rule, Credit Information Companies (Regulations) Act 2005, Indian Telegraph Act, 1885, Telecom Regulatory Authority of India act, 1997, Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act-2016.

In "The constitution of India" has some provisions like, 'Freedom of Speech and Expression' and 'Right to Life and Personal Liberty' These provisions have its effect to the right to privacy as a fundamental right. There are number of cases also which establishes the right to privacy as a fundamental right. The conceptuality of this proposition has also connected with the new dimension of the 'Data Protection'. The linkage between this privacy and data protection are interdependent to each other. The right of data protection is the closely related with the 'information' of an individual.

In case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others*** decided that the decision of ***M P Sharma v Satish Chandra, District Magistrate, Delhi*** and ***Kharak Singh v State of Uttar Pradesh***, is over-ruled and decided that the "The right to privacy is protected as an intrinsic part of the right to

life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

The Right of Privacy is a fundamental right. It is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices.

At the national level "The Information Technology Act, 2000" ("IT Act") was the first law enacted in India which contained provisions on confidentiality, privacy and security for information stored in a computer resource. In 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Data Protection Rules") were enacted under the IT Act to protect sensitive personal data and information collected from individuals by body corporates. These rules make up the existing general data protection framework in India.

The Government has provided a legal framework for data protection and privacy through the IT Act and the IT Rules.

Section 43 of this IT Act provides provision related to Penalty and compensation for damage to computer, computer system, etc. Section 43-A provides provision related to Compensation for failure to protect data. Section 66-C provides provision related to Punishment for identity theft. Section 66E is of utmost importance. Privacy violation of a person without his consent has been made punishable by virtue of this provision. It provides provisions related to Punishment for violation of privacy. Section 72 provides provisions related to Penalty for Breach of confidentiality and privacy. Section 72-A provides that, when 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 Five Lakh rupees, or with both.

Rule 4, 5, 6,8, of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011provides provisions related to Data Privacy protections.

In the, “The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016” The objective of this Act, to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto.

Section 28,29,30,33 of the “The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016” (Aadhaar Act) provided provisions related to the Data protections of the data subjects.

Sections 28 of this Act provide that it is the duty of the authority, to take all necessary measures to ensure that the information in the possession or control of the authority, including information stored in the Central Identities Data Repository, is secured. This type of information’s is protected against access, use or disclosure not permitted under the Aadhaar Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage. Section 29, prohibits the sharing of core biometric information which collected or created under the Aadhaar Act, with anyone for any reason; or be used for any purpose other than generation of Aadhaar numbers and authentication under the Aadhaar Act.

Researcher analysis different themes highlighted data protection has treated as a right on different perspective. All the Subjects like right to privacy, right to information, information technology, corporate affairs and consumer were giving special emphasis to accept the fact data protection as a right. It is required strengthening data protection regime for the protection of individual liberty. To give special status to data protection as a right, the facets of data protection like data collection, processing, storage, security and access should provide a platform together in legal framework. The awareness about the right base approach of data protection and privacy has to spread worldwide unanimously.

Chapter III- Impact of Social Media on Data Privacy

In this chapter I discussed that how social media impact on our data privacy. I also discussed what is social media? Social Media are a tool that have change the way people communication. Word “Social Media” is combination of two word, first

"Social" and second 'Media". The word "Social" refers to interacting with other people by sharing information with them and receiving information from them.

The word "Media" refers to an instrument of communications or tools of communications. So, we say that Social Media are web- based communication tools that enable people to interact with each other by both sharing and consuming information.

I also discussed Types of Social Media like SNSs (Social networking sites), Blogs, Facebook Inc., Tweeter, LinkedIn, Google+, YouTube, WhatsApp Messenger, Google Maps, Zoom Cloud Mitting, Arogya Setu Apps, Ola /Uber Apps, etc. In this chapter I discussed that Data Privacy Threats like Clickjacking, De-anonymization Attacks, Fake Profiles, Information Leakage, Location Leakage etc. in this chapter also discussed that positive and negative impact of these social media on Educations, politics, society, youngster, etc.

Chapter IV- COMPARATIVE ANALYSIS OF "THE DATA (PRIVACY AND PROTECTION) BILL, 2017" AND "THE PERSONAL DATA PROTECTION BILL,2018"

In this chapter I discussed the Comparative analysis of the "The Data (Privacy and Protection) Bill. 2017" and "The Personal Data Protection Bill,2018".

The Data (Privacy and Protection) Bill, 2017 is an effort to protect the Data Privacy of an individual person.

This Bill provides for a framework to address the issue on data protection and protect the privacy of all persons. This Bill is Introduced in Lok Sabha in September 2017 by the SHRI BAIJAYANT PANDA. The Objective of this Bill to codify and safeguard the right to privacy in the digital age and constitute a Data Privacy Authority to protect personal data and for matters connected therewith. It intends to provide rights of persons vis-a-vis their own information, as well as procedures for data collection, data processing, reasonable and targeted surveillance, and means of redress in case of breaches and violations.

In light of this Bill, while the collection and processing of data is important, there is an overwhelming need to secure personal data and ensure better security by creating a statutory obligation to safeguard data and individuals.

The Bill seeks to codify and safeguard the right to privacy for all juristic persons in the digital age, balanced with the need for data protection in the interests of national security.

This bill was divided into IX Chapter and two Schedule. This bill was provided the law related to the data privacy in India. This bill defines the Data, Personal Data, Sensitive Personal Data, Anonymized Data, Person, Authorised Officer, Data processing Data Controller, Data Processor, Third Party etc

Chapter II dealt the "Rights of the Data Subjects", these are fallowing mentions-

- Right to Privacy
- Right to Secure Personal Data
- Right to Accessed Personal Data
- Right to Rectification of Personal Data
- Right to Removal of Personal Data

Chapter IV of the Bill of 2017, dealt the transfer, storage, and security of personal data. This chapter provide that prohibition of sharing of personal data, retention of personal data, prohibition of unnecessary storage of personal data transfer of personal data to third party, cross-border transfer of personal data, etc.

Chapter V dealt with the obligation of data controller and processer. Provision related to responsibility of data controller or processer mentation in this chapter that that is, to Collection of personal data in fair and lawful manner, to maintain confidentiality, to take adequate measure for fortification, to maintain accurate records etc.

Chapter VII dealt the "Data Privacy Authority". This chapter provide provision related to constitution of data privacy authority, appointment of chairperson and other member, procedure and power of authority, filing of complaints, appeal, etc.

Chapter VIII of this Bill dealt the provisions related to "Offences and Penalties". In this chapter provide provision related to punishment for offence related to personal data and sensitive personal data, breach of confidentiality and security, penalty for contravention of direction etc.

Every offence under this Act treated as Cognizable offence. When any person non-compliance the provision of this Act, collect, storage, receive, processes, publishes, or otherwise handle personal data shall be punishable with a term which may extent to five years imprisonment and fine which may extend up to rupees fifty thousand for each day of unlawful access to the personal data.

The Personal Data Protection Bill, 2018"

After the case of Justice **K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others** the Government of India has set up Committee of Experts to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill. The objective is to "ensure growth of the digital economy while keeping personal data of citizens secure and protected." Justice B. N. Krishna (Bellur Narayanaswamy Krishna), former judge of the Supreme Court of India is the head of Expert Committee. The government led Nine-member committee to "identify key data protection issue in India and recommended methods of addressing them". Justice B.N. Krishna Committee has put out a "White Paper on Data Protection Framework for India". This White Paper has been drafted to solicit public comments on what shape a data protection law must take. etc. In white paper seven key principles on Data Protection proposed by the expert committee, these are, Technology Agnostic, Holistic Application, Informed Consent, Data Minimisation, Controller Accountability, Structured Enforcement, Deterrent Penalties.

After the analysis and discussion of "white Paper on Data Protection Framework for India" Justice B. N. Krishna Committee submit his final report on data privacy and submitted draft of "Personal Data Protection Bill,2018" to the Government. This Bill will from the framework for India's Data Protection law's Prescribing how Organization should collect, process and store citizens Data. This is a keystone development in the evolution of data protection law in India. With India moving towards digitization, a robust and efficient data protection law was the need of the hour. The Bill has been drafted with an intention to fill in the vacuum that existed in the current data protection regime, and to enhance individual rights by providing individuals full control over their personal data, while ensuring a high level of data protection.

The Bill has been broadly based on the framework and principles of the General Data Protection Regulation (GDPR) recently notified in the European Union.

The Personal Data Protection Bill,2018 is divided into fifteen Chapters and two Schedule. Schedule II related to the "Amendment to the Right to Information Act,2005" and Schedule I related to the "Amendment to the Information Technology Act, 2000".

Chapter II of the "The Personal Data Protection Bill,2018" provided principles related to data protection. The data protection principal originally derived from the council of Europe Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data. The principles of the convention were also implemented in the Data Protection Act, 1984 and consequently, the data protection principles contain in the Data Protection Act,1998. These principles are the backbone of the data protection law. This principal is also provided in the "The Personal Data Protection Bill.2018". The objective of these principles is to protect the interest of the individuals whose personal data is being processed. These are the principles

(1) Fair and reasonable processing principles
(2) Purpose limitation principles
(3) Lawful processing principles
(4) Notice and choice principles
(5) Data quality principles
(6) Data storage limitation principles
(7) Accountability principles

Chapter III, IV, V of this Bill dealt the provision related to Processing of Personal Data. Chapter III dealt the provision related to the Personal Data. Chapter IV dealt the provision related to the Sensitive Personal Data. While Chapter V dealt the provision related to the Processing of Personal Data and Sensitive Personal Data of children.

Chapter VI of this bill provide provision related to the data principal rights. In order to ensure a robust data protection law, it is essential to provide data principals with the means to enforce their rights against corresponding obligations of data fiduciaries. These rights are based on the principles of autonomy, self-determination, transparency and accountability so as to give individuals control over their data,

which in turn is necessary for freedom in the digital economy. A strong set of data principal rights is an essential component of an empowering data protection law.

Bill provided the fallowing rights of the data principal, that is

(a) Right to confirmation and access
(b) Right to correction
(c) Right to data portability
(d) Right to be forgotten

Chapter VII of this bill provide provision related to "Transparency and Accountability Measure". In this chapter, provide provision related to the duty and obligation of data fiduciary. In this regards fallowing duty and obligations of data fiduciary are provided, that is,

(a) Maintain data Privacy
(b) Maintain Transparency
(c) Maintain Security Safeguards
(d) Personal Data Breach Notification
(e) Maintain Personal Data Record
(f) Appointment of data protection officer
(g) Provide Grievance

Above mention obligation and duty of data fiduciary is important for data protection. Without these duty or obligation of the data fiduciary we cannot achieve the objective of this bill.

Chapter VIII of this bill provide provision related to "Transfer of Personal Data Outside India".

It is essential to ensure that the interests of effective enforcement of the law, economic benefits to Indians need to be core to any proposed framework for cross-border transfer. However, these must not unjustifiably impede international flow of personal data, which itself is beneficial in many ways for Indians. This is similar to the physical economy in India where a combination of free movement of goods and transfer restrictions operate alongside each other.

Chapter IX of this bill dealt the provision related to exemptions.

For the creation of a truly free and fair digital economy, it is vital to provide certain exemptions from obligations that will facilitate the unhindered flow of personal data in certain situations. These exemptions derive their necessity from either a state or societal interest. However, these exemptions must be limited to processing that is necessary and proportionate to the purpose sought to be achieved. In this bill carefully outline watertight exemptions that are narrow and are availed in limited circumstances. Further, adequate security safeguards must be incorporated in this bill to guard against potential misuse.

This chapter dealt the fallowing Exemption, that is

(a) Security of the state
(b) Prevention, detection, investigation and prosecution of contraventions of law
(c) Processing for the purpose of legal proceeding
(d) Research, archiving or statistical purposes
(e) Personal or domestic purposes
(f) Journalistic purposes
(g) Manual processing by small entities

Chapter X of this bill dealt the provision related to the Data Protection Authority of India. In this chapter provided fallowing provision

(a) Establishment and incorporation of authority
(b) Composition and qualification for appointment of members, Removal of members
(c) Power and Functions of the authority
(d) Power of authority to issue direction
(e) Power of authority to call for information

Chapter XI of this bill, provide provision related to the "Penalties and Remedies" for the violation the provision of this bill.

An appellate tribunal shall be set up to hear and dispose of any appeals from the orders of the Data Protection Authority and the orders of the Adjudicating Officers under the Adjudication Wing of the DPA. Such a tribunal should consist of a chairperson and such number of members as notified by the Central Government. The Central Government may also confer powers on an existing tribunal for this purpose if it believes that any existing tribunal is competent to discharge the functions of the

appellate tribunal envisaged under the data protection law. The orders of the appellate tribunal will be finally appealable to the Supreme Court of India.

Chapter XIII dealt the provision related to the offences.

Comparative analysis

The Personal Data Protection Bill, 2018 (Bill of 2018) is wider than The Data (Privacy and Protection) Bill,2017 (Bill of 2017). In the Bill of 2018 right to data privacy is recognized as fundamental right, while the Bill of 2017 data privacy is not recognized as fundamental right. In the Bill of 2017, the Word "Data" define in very limited sense, while the word data define in bill of 2018 in wider sense. In the bill of 2018, data includes a representation of information fact concepts opinion, interpretation, or processing by humans or automated means. In the bill of 2017, word "Person" defines in very limited sense. In this bill word person only includes the individual. While, in the bill of 2018, word "Person" includes the an individual, a Hindu Undivided family, a Company, a firm, a State, an association of person, every artificial juridical person. So, the definition of the person in the bill of 2018 is wider than definition given in the bill of 20017. In the bill of 2018 "Data Fiduciary" is come on place of "Data Controller". Some important provision provides in the bill of 2018 that is,

(1) Data Protection Principles, which is apply on any type of data processing. Where the data fiduciary or data processer violation of these principles there he is liable for penalty.

(2) "Right to be Forgotten" or "the right to be erased" allow an individual to request for removal of his personal information /data online.

(3) Bill provides excessive powers to the central government, to issue direction in certain circumstances, especially under Section 98.

(4) Bill provides provision related to data principals right, such as Right to Access, Right to Correction, Right to Data portability, etc.

(5) Provides provision related to cross- border transfer of personal data and sensitive personal data.

(6) Provide provision related to appointment of Data Protection Authority, power and function of the authority, Appointment of adjudicating officer, etc.

(7) Provide provision related to appeal to the Appellate Tribunal, Appeal to Supreme Court of India

(8) Providing Penalty and remedies for the violation of the provision of this Bill.

This Bill is applied to processing of personal data and Sensitive personal data. Sensitive personal data include financial data, health data, biometric data, genetic data, etc.

In the bill of 2017, matter related to the data privacy is decided by the bench. That bench is constituted by the Data Privacy Authority. While, in the Bill of 2018 matter related to data privacy dealt by the Adjudicating Officer or Adjudicating wings. Adjudicating officer or Adjudicating wings are appoint by the Data protection Authority accordance in the Bill of 2018.

In the "The Data (Privacy and Protection) Bill,2017, provide provision for appeal in limited sense. In this Bill appeal against the decision of the bench, lie to the Telecom Disputes Settlement Appellate Tribunal. Which is set up in accordance with the provision of the Telecom Regulatory Authority Act, 1997. There is no provision for appeal to Supreme Court. While, in the "The Personal Data Protection Bill,2018" provide provision for Appeal in wider sense. In this Bill, where any adjudicating officer issue order or given decision, in data privacy matter then the party, who suffering from such decision or order have right to appeal to the Appellate Tribunals. Parties have right to go to Supreme Court of India against the decision of Appellate Tribunal.

Chapter V- Judicial Travelling on the Issue of Privacy and Data Protection

In this chapter I discussed the judicial decision given by the Indian courts, European courts, Human Rights Court, European Courts of Human Rights, etc. I also discussed that how judiciary play a vital role for the protection of data privacy. In this chapter I discussed that Indian Judiciary play a vital role for the protection of "Privacy" and "Data Protections". The existing law just affords a principle which if properly invoked may protect the privacy of the individual. Indian judiciary has been using judicial activism to widen the ambit of the Article 21 of the Constitution of India. Where the seeds of the privacy right may be found. The journey began in 1963,

when for the first time the issue regarding right to privacy was raised in **Kharak Singh v. state of UP**.

The movement towards the recognition of right to privacy in India started with **Kharak Singh vs The State of U.P**. The question for consideration before this court was whether 'surveillance' under Chapter XX of the U.P. Police Regulations constituted an infringement of any of the fundamental rights guaranteed by Part III of the Constitution. Regulation 236(b) which permitted surveillance by 'domiciliary visits at night' was held to be violative of Article 21.

Supreme Court held that "An unauthorized intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common law right of a man —an ultimate essential of ordered liberty, if not of the very concept of civilization".

In a minority judgment in this case, Justice Subba Rao held that "the right to personal liberty takes is not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty.

In 1972, the Supreme Court, In **R. M. Malkani vs State of Maharashtra** case, the petitioner's voice had been recorded in the course of a telephonic conversation where he was attempting blackmail. He asserted in his Defence that his right to privacy under Article 21 had been violated. The Supreme Court declined his plea holding that "the telephonic conversation of an innocent citizen will be protected by courts against wrongful or high-handed interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants."

Further in **Govind vs. State of Madhya Pradesh** the decision by a three-judge bench of the Supreme Court is regarded as being a setback to the right to privacy jurisprudence. Here, the court was evaluating the constitutional validity of Regulations 855 and 856 of the Madhya Pradesh Police Regulation which provided for police surveillance of habitual offenders including domiciliary visits and picketing. The Supreme Court desisted from striking down these invasive provisions holding that "It cannot be said that surveillance by domiciliary visit, would always be

an unreasonable restriction upon the right of privacy. It is only persons who are suspected to be habitual criminals and those who are determined to lead criminal lives that are subjected to surveillance."

In the case of **R. Rajagopal vs. State of Tamil Nadu.** In the case involved a balancing of the right of privacy of citizens against the right of the press to criticize and comment on acts and conduct of public officials.

Supreme Court held that "The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, motherhood, education among other matters. No one can publish anything concerning the above matters without his consent- whether truthful or otherwise and whether laudatory or critical

In the case of **PUCL vs. Union of India** the court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right to privacy. The Supreme court held that,

The matter of telephone tapping reiterated that right to privacy was part of the right to life and personal liberty enshrined in Article 21 of the constitution and included the 'telephone conversation in the privacy of one's home or in office as right to privacy'. Telephone tapping would thus infract Article 21 of the Constitution unless it was permitted under the procedure stablished by law.

The Supreme Court decision in Smt. **Selvi & others. v. State of Karnataka** is a welcome development in respect of protection of privacy. In which the court held that Norco, Polygraph and Brain Mapping tests can no more be conducted on anyone, either an accused or a suspect, without his/her consent. A bench of Chief Justice K.G. Balakrishnan and Justices R.V. Raveendran and J.M. Panchal said that the forcible administration of these tests was "an unwarranted intrusion into the personal liberty" of those facing criminal offences." No individual should be forcibly subjected to any of the techniques in question, whether in the context of investigation in criminal cases or otherwise. Doing so would amount to an unwarranted intrusion into personal liberty.

Finally, Supreme Court of India in case of Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others decided that the decision of M P Sharma v Satish Chandra, District Magistrate, Delhi and Kharak Singh v State of Uttar Pradesh, is over-ruled and decided that the "The right to privacy is protected as an intrinsic part

of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

In the case of Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others supreme court observed that,

"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."

For this Purpose, Government of India has set up Committee of Experts to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill. The objective is to "ensure growth of the digital economy while keeping personal data of citizens secure and protected." Justice B. N. Krishna (Bellur Narayanaswamy Krishna), former judge of the Supreme Court of India is the head of Expert Committee. The government led Nine-member committee to "identify key data protection issue in India and recommended methods of addressing them".

In Indian law, the right of Data Privacy is in its infant stage. It is just present in Article 21 of the Constitution of India. There is an urgent need for the law to address such lacunas.

Chapter VI- Reporting Research Findings

In this chapter researcher collected data and analyzed that data. In this analysis researcher find out that what is the problem arise in data privacy and their protections. For the purpose of this chapter and fruitful research on the research topic, researcher make a questionnaire for collection of data. Research collect data from UG, PG, Students, Research Scholars, Assistant Professors, Associate Professors, Professors and lay man. Researcher fill-up 205 questionnaire. All respondent respond carefully and some respondent give some suggestion. For the purpose of data collections researcher put total 22 questions in their questionnaire.

After the analysis of these 22 Chart researchers find out that, In India maximum number of persons are android Mobile user. They use internet in their daily

progressive life. For their daily progressive life they use Swigi, Zomato, Ola, Uber, Amazon, Flip cart, Big basket, Grosser Apps, Facebook, Instagram, Tweeter, etc. they are use different social Networking sites, different social media apps in daily, they spend time on these social media and different Social networking sites in more than 5 hours daily. But they not read carefully term and policies of that SNSs and social media Apps. Due to this reasons Data privacy breach of Data users. Maximum user doesn't know about "Privacy" become fundamental rights in Indian Constitution. They don't about the "The Personal Data Protection Bill,2018". They don't about the Personal Data, Sensitive Personal Data, Rights of Data Users, what remedies available for the breach of data privacy.

So, its required that aware the people for their data privacy Rights, aware about the what remedies available and where remedies available for the breach of data privacy. Draft a special Act for the protection of data privacy. Constitute data privacy protection tribunals in every state, and district level for speedy justice.

Chapter VII- Concluding Remarks

(a) Conclusion
(b) Suggestions

In this chapter researcher reached this conclusion that In India, different themes highlighted data protection has treated as a right on different perspective. All the Subjects like right to privacy, right to information, information technology, corporate affairs and consumer were giving special emphasis to accept the fact data protection as a right. The purpose of the problem is strengthening the outlook of data protection as a right in this technological liberalization age. The scope of technology day by day increasing to maintain this increasing phenomenon, it is requiring strengthening data protection regime for the protection of individual liberty. Idea to have this research work is to establish right to privacy and data protection right as a processing, storage, security and access should provide a platform together in legal framework. The awareness about the right base approach of data protection and privacy has to spread worldwide unanimously.

On comparing the Indian law with the law of developed countries the proper requirement for the Indian law can be analyzed. Data are not of same utility and

importance; it varies from one another on the basis of utility. So, we require framing separate categories of data having different utility values, as the U.S have. Moreover, the provisions of IT Act deal basically with extraction of data, destruction of data, etc.

A right to protect one's data on online platforms constitutes data privacy. Such data could either be concerned with an individual, enterprise or even a government. Personal information provided by individuals during biometrics also included in data. But data put out through biometrics or for economic purposes remains at risk in India since no legislation has been chalked out to protect such personal data.

Despite the efforts being made for having a data protection law as a separate discipline. In India it is required that bill has been drafted wholly on the structure of the UK Data Protection Act whereas today's requirement is of a comprehensive Act. Institutional status of data protection can give a universal approach to data protection. To give special status to data protection as a right, the facets of data protection like data collection, Thus, it required that a compiled drafting on the basis of US and UK laws relating to data protection would be more favorable to the today' requirement.

In view of the above observations, few Suggestions may be put forward in order to provide appropriate remedy in the cases of Data Privacy violation. As such the following Suggestions may be cited,

(1) In India, Right to Privacy has been established as Fundamental Right under Article 21 of the Indian Constitution by way of judicial activism only. This has continued the debate on the recognition of Right to Privacy as a Fundamental Right, which can only be ended by incorporation of it as a Fundamental Right through constitutional amendment. Therefore, a new article, called Article 21B should be inserted with a title "Right to Privacy" in the Part-III of the Indian Constitution.

(2) Constitutional protection for Right to Privacy and Data Privacy is not enough, statutory protection of it is also required. As such, a full-proof statute on Data Privacy should be enacted. In this respect, the long-standing "The Personal Data Protection Bill, 2018" should be passed into an Act, otherwise strong punishment cannot be provided in the cases of Privacy violation.

(3) Some loop hole found in "The Personal Data Protection Bill, 2018" in India; In this Bill Data Principal have "Right to Access" his personal data in this

Bill. In this regards time period is not prescribed for this right. In within how much time data fiduciary hand over the brief summary of the processing of personal data or sensitive personal data, to the Data Principal. Though it is a very serious problem and should be prevented, but the other cases of loss of Personal Data should be taken into account by the Indian Legislature.

(4) When any person collects personal data of any persons, there must be strict data collection policy imposes by the top authority on that authority which collect data. In policy its clearly mention that,

a) Information is collected by authorize appointed agency only.

b) Information is collected for lawful purpose only.

c) Personal data shall be adequate, relevant and not excessive.

d) Purpose of information collection must be mention.

(5) Government should authorize the proper agencies for data collection.

(6) Authorized agency when they collect data, information etc. it must be collected for lawful purpose only, its commercial use is strictly avoided.

(7) Appropriate technical and organizational measure shall be applied for the store of personal data. Collected personal data shall be kept accurately and kept up-to-date. Use all Technical measures include all information security controls which are necessary to keep information security over internet.

(8) When personal data store on the server then that server must be fully controlled by Appropriate government. Server must be taken all security safeguard against unauthorized access, use and other modification.

(9) when the processes of personal data on the consent of the data user then Data Processor shall adopt the fair and lawful processing of Personal data. After processing, the data must be properly disposed.

(10) Its internet era, every office school college, company, government office, Indian Army, Bank, Railway, Airlines, Treasury office, malls, etc. every use internet for their progressive work. Hacker use internet and hacks our personal data that we share on these offices. So, its required that expert make a special software which is not hacked by the hackers.

(11) Governmental and non-governmental agency collect our personal data by different mode. They share our personal Data to various company withought the prior permission of the data Principal. So, its required that when

any Governmental or non -governmental agency or any company share personal data of the data principal to any one, then firstly these company or governmental or non- governmental agency to inform the data principal that they want share their personal data for specific purpose and they wants receive their consent for share their personal data.

(12) It is required that the Data Protection Officer, Adjudicating Officers, Appellate Tribunals are stablished in Every District level for the protection of Data Privacy.

If the above suggestions are implemented through appropriate measures, it is sincerely hoped that the right to Data Privacy can be protected more effectively.