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

**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

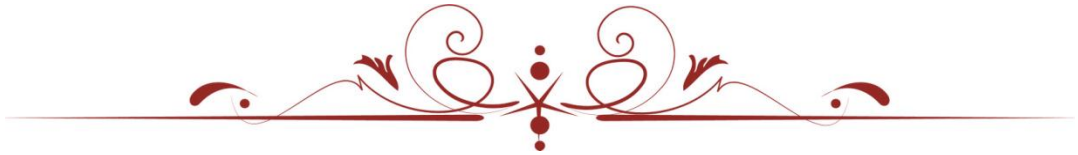

**SUPERVISOR**
**PROF. PRITI SAXENA**
**DEPARTMENT OF HUMAN RIGHTS**

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



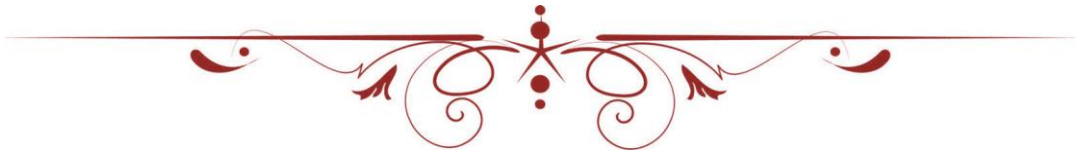
**DEPARTMENT OF LAW**
**SCHOOL FOR LEGAL STUDIES**
**BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY**
**(A CENTRAL UNIVERSITY)**
**VIDYA VIHAR, RAEBARELI ROAD**
**LUCKNOW-226025**


**2020**



*Dedicated to*

*My Beloved Parents*



BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

बाबासाहेब भीमराव अम्बेडकर विश्वविद्यालय
(केन्द्रीय विश्वविद्यालय)
विद्या विहार, रायबरेली रोड, लखनऊ–226025
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
Vidya Vihar, Raebareli Road, Lucknow-226025
**Accredited 'A' Grade by NAAC in 2015**

**Letter No:**
**Date:** 27/10/2020

# DECLARATION

I, **Arun Kumar Mishra**, hereby declare that this research work for the award of Ph.D. degree entitled **"A Study on Judicial Trends in Privacy Law with Special Reference to Data Protection"** has been done by me on the basis of original research material and information taken from other research works has been duly acknowledged.

I further declare that this is an original work and has not been previously submitted in part or full for any other degree or diploma in this or any other university.

Mishra

**Dated:**
**Place:**

**(Arun Kumar Mishra)**
Research Scholar
Department of Law
School for Legal Studies
Babasaheb Bhimrao Ambedkar University
Lucknow-226025 (U.P)

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

बाबासाहेब भीमराव अम्बेडकर विश्वविद्यालय
(केन्द्रीय विश्वविद्यालय)
विद्या विहार, रायबरेली रोड, लखनऊ–226025

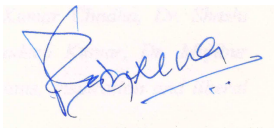
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
Vidya Vihar, Raebareli Road, Lucknow-226025
**Accredited 'A' Grade by NAAC in 2015**

**Letter No:**
**Date:** 27/x/xx

# CERTIFICATE

This is to certify that the thesis titled **"A Study on Judicial Trends in Privacy Law with Special Reference to Data Protection"** Submitted by Mr. **Arun Kumar Mishra** is an original research work and has not been previously submitted in part or full for the award of any other degree or diploma to this or any other university.

The thesis submitted to Babasaheb Bhimrao Ambedkar University satisfies all the requirements as stipulated in the *Doctor of Philosophy (Ph.D.) regulations-1999 as amended in 2013* and it is fit for submission and evaluation for the award of the degree of Doctor of Philosophy of the University.



**Date:** 27/x/xx

**Supervisor**

**(Prof. Priti Saxena)**

**Head**
**Department of Law**
**School for Legal Studies**

# ACKNOWLEDGEMENT

*The present attempt is directed by the supernatural power, which awakened to be endowed with the prestigious task of accomplishing the work in hand. On the occasion of submission of this thesis first and foremost, I would like to express my deepest sense of gratitude to Almighty for his loving care and enabling me to accomplish this venture.*

*With an utmost degree of sincerity, I avail this opportunity to express my heartfelt thanks to my learned guide and supervisor* ***Prof. Priti Saxena, Department of Human Rights, School for Legal Studies, BBAU, Lucknow*** *for his keen interest, valuable guidance, consideration, criticism and unceasing encouragement throughout the thesis work without his interest and deep involvement my thesis could not have been successfully completed.*

*I wish to express my deep sense of gratitude to Prof. Sudarshan Verma, Head and Dean, Department of Law, School for Legal Studies, BBAU, Lucknow for permitting me to work on this topic and his active support and all the facilities provided by him in this regard.*

*I take this opportunity to express my deep sense of gratitude to my respected teachers of the, School for Legal Studies, BBAU, Lucknow, namely, Prof. Sanjeev Kumar Bhatnagar, Prof. Preeti Mishra, Dr. Sanjeev Kumar Chadha, Dr. Shashi Kumar, Dr. Sufia Ahamed, Dr. Anis Ahmad, Dr. Pradeep Kumar, Dr. Mujibur Rehman. Dr. Rashida Ather, for their valuable suggestions, inspiration and liberal help rendered during the course of research.*

*I have no words to express my gratitude to my mother Smt. Pushpa Mishra and my father Shri Prem Narayan Mishra for their blessing affection and moral support throughout my study. I must also acknowledge my gratitude to my family members viz. my brothers Dr. Abhishek Kumar Mishra (Veterinary Officer, UP) and Naveen Kumar Mishra (Assistant Manager, State Bank of India), Deendayal Mishra, Vishal Mishra, Shiv Kumar, Nutan, my sisters-in-laws Smt. Ranjana Mishra and Smt. Pratibha Mishra, my Sisters Smt. Neetu Mishra and her husband Arvind Kumar Mishra, Smt. Ragini Mishra and her husband Shashikant Pathak, and my Nephews*

*and Nieces viz Abhinav, Arpit, Arnav, Aarush, Shivangi, Atharv Mishra and Anaya Mishra for their love and affections.*

*I am deeply thankful to my seniors Dr. Rajeev Kumar Singh. Dr. Munis Swaroop, Dr. Girijesh Singh, Dr. Vijay Bhaskar, for their possible help during the course of research and preparation of thesis.*

*I am deeply thankful to my friends Satyendra Maurya (Judicial Magistrate U.P), Neha Singh (Judicial Magistrate Bihar), Neeraj Verma (DHO, UP), Manindra Kumar Singh (Assistant Professor), Anil Kumar (Research Scholar) Sateesh Kumar(Research Scholar), Pramod Kumar (Research Scholar), Rajit Ram Sonkar (Research Scholar), Ajit Kumar Gond (Research Scholar), Veer Vikram Bahadur Singh (Research Scholar), Pankaj Gupta, Harinandan Pandey (Advocate), Anurag Tripathi (Advocate), for their possible help during the course of research and preparation of thesis.*

*I express my thanks to all the Clerical staff of the School for Legal Studies, BBAU, Lucknow viz. Awadhesh Yadav, Anil Srivastava, Dharmendra, Kamruddin, Atik, for helping me in availing all the facilities required for this work.*

*I express my thanks to all the library staffs, Department of Law and Library staffs of the Gautam Buddha Central Library, BBAU, Lucknow, Lucknow University and RML University, Lucknow for helping me in availing all the facilities required for this work.*

*Last but not the least, I am also thankful to the Dr. Swadesh Kumar proprietor of Scholar Hub, Ratanakarkhand, Southcity, Lucknow, for transforming the manuscript into the present form.*

Mishra

***(Arun Kumar Mishra)***

## Chapter I

## Introduction

**Content** **Page No.**



## Chapter II

## Right to Privacy and Data Protection

**Part A : International Perspective**

## *Chapter II*

## Right to Privacy and Data Protection

**Part 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 Traveling on the Issue of Privacy and Data Protection

## Chapter VI

## Reporting Research Findings

## Chapter VII

## Concluding Remarks



## Annexure

# Case Law List

1. **U.S.A Case Law:**

- Bowers v. Hardwink [478 U.S. 186 (1986)]
- Boyd v. United States [116 U.S. 616(1886)]
- Burger v. New York [388 U.S. 41 (1967)]
- Frank v. Maryland' [359 U.S. 360 (1959)]
- Katz v. United States [389 U.S. 347 (1967)]
- Mapp v. Ohio [367 U.S. 643(1961)]
- Olmstead v. United States [277 U.S. 438 (1927)]
- Planned Parenthood of Southern Pennsylvania v. Casey [112 S. Ct. 2791(1992)]
- Planned Parenthood v. Danforth [428 U.S. 52 (1976)]
- Webseter v. Reproductive Health [109 S. Ct 3040 (1989)]
- Wolf V. Colorado. [338 U. S. 25 (1949)]

2. **U.K Case Law:**

- Kaye v. Robertson [(1995) 1 WLR 804]
- Pollard v. Photographic Co [40 Ch. D 345 (1888)]
- Prince Albert V. Strange [41 ER 1171 (1849)]
- Tudc v. Priester [19 Q.B.D]
- Wilkinson v. Downton, [(1887) 2 Q.B, 57]

3. **Indian Case Law:**

- Amar Singh v Union of India [(2011) 7 SCC 69]
- Bhabani Prasad Jena v. Orissa State Commission for Women [ (2010)8 SCC 633]
- Board of Revenue, Madras v. R. S. Jhawar [AIR 1968 SC 59]
- Directorate of Revenue v. Mohammad Nisar Husain [AIR 2008 SC 524]

- District Registrar and Collector, Hyderabad v. Canara Bank [AIR 2005 SC 186]
- Govind vs. State of Madhya Pradesh [(1975)2 SCC 148]
- In T. Sareetha v. T. V. Subbaish [AIR 1983 AP 356]
- K. S. Puttaswamy (Retd.) v Union of India [2017(10) SCALE 1]
- K. S. Puttaswamy and Others Vs. Union of India [2017(10) SCALE 1]
- Kharak Singh vs The State of U.P. [AIR 1963 SC 1295].
- M.P Sharma v. Satish Chandra [AIR 1954 SCR 1077]
- Malak Singh v. State of Punjab & Haryana [AIR 1981 SC 760]
- Mr. Ansari Masood A.K v. Ministry of External Affairs [(2010) 9 SCC 152]
- Mr. 'X'. Vs. Hospital Z [AIR 1999 SC 495]
- Naz Foundation v. Government of NCT of Delhi
- Neera Mathur v. LIC of India, [AIR 1992 SC 392]
- Nihal Chand v. Mt. Bhagwan Devi [AIR 1935 All 1002]
- PUCL vs. Union of India [AIR 1997 SC 568]
- R. M. Malkani vs State of Maharashtra [AIR 1973 SC 157]
- R. Rajagopal v. State of Tamil Nadu [AIR 1995 SC 264]
- R.C. Cooper v UOI [(1970) 1 SCC 248]
- Ram Jethmalani & Others v. Union of India, [ (2011) 8 SCC 1]
- Sarda v. Dharmpal, [AIR 2003 SC 3450]
- Selvi v. State of Karnataka [(2010) 7 SCC 283]
- Smt. Rayala M. Bhuvaneshwari v. Nagaphanender Royals, [AIR 2008 A P 98]
- State of Karnataka v. Krishnappa [AIR 2000 SC 1470]
- State of Maharashtra v. Bharat Shanti Lal Shah [(2008) 13 SCC 5]
- State of Maharashtra v. Madhukar Narayan Markikar, [AIR 1991 SC 207]
- State of Punjab v. Baldeo Singh [AIR 1999 SC 2378]
- State of Punjab v. Baldeo Singh [AIR 1999 SC 2378]
- Suchitra Srivastava and another's v. Chandigarh Administration [(2009) 9 SCC 1]
- V.S. Kuttan Pillai v. Ramakrishna [AIR 1980 SC 185]
- Vandana Kumari v. P Praveen Kumar [AIR 2007 AP 17]
- Vijay Prakash v. Union of India [AIR 2010 Delhi 7]
- Yusuf Ali Ismail Nagree v. State of Maharashtra [AIR 1973 SC 15]

# Abbreviations

| | | |
|---|---|---|
| A.C | : | Appeal Cases |
| ACHPR | : | African Charter on Human and People's Right. |
| ACHR | : | American Convention on Human Rights. |
| ADRDM | : | American Declaration of the Rights and Duties of Man. |
| AIR | : | All India Reporter |
| AIR(SC) | : | All India Reporter (Supreme Court) |
| AIR (J) | : | All India Reporter Journals |
| A.J.C. L | : | American Journal of Comparative Law |
| A.J.I. L | : | American Journal of International Law |
| ALT | : | Allahabad Law Times |
| Alld. | : | Allahabad |
| A.L. J | : | Australian Law Journal |
| ALR | : | American Law Reports |
| AAL R | : | Anglo-American Law Review |
| All. E. R | : | All England Law Reports |
| All ER (EC) | : | All England Law Reports (European Cases) |
| All ER Rev | : | All England Law Reports Annual Review |
| All L J | : | Allahabad Law Journal |
| All L R | : | Allahabad Law Reports |
| All L T | : | Allahabad Law Times |
| Ala L Rev | : | Alabama Law Review |
| ALT | : | Andhra Law Times |
| A.L.J. R | : | Australian Law Journal Reports |
| Am U L Rev | : | American University Law Review |
| APEC | : | Asia Pacific Economic Corporation |
| APQ | : | American Philosophical Quarterly |
| Art. | : | Article. |
| ASIL | : | American Society of International Law |

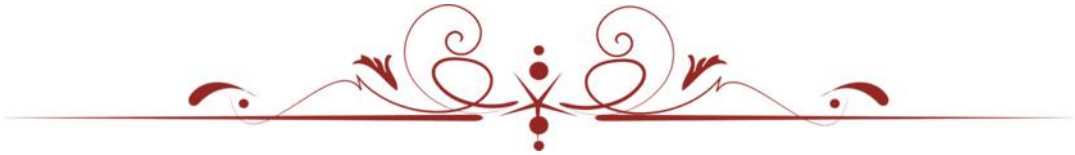
| | | |
|---|---|---|
| B.C.L. R | : | British Columbia Law Reports |
| BLJ | : | Banaras Law Journal |
| BLR | : | Bombay Law Review |
| BJLS | : | British Journal of Law and Society |
| Bom. | : | Bombay |
| B.Y.I. L | : | British Yearbook of International Law |
| Can. B. R | : | Canadian Bar Review |
| C.A | : | Court of Appeal |
| CESCR | : | Committee of Economic, Social and Cultural Rights |
| C.A. D | : | Constituent Assembly Debates |
| CIC | : | Credit Information Companies |
| C.J. I | : | Chief Justice of India |
| CLT | : | Cuttack Law Times |
| C.L. J | : | Cambridge Law Journal |
| Cal. | : | Calcutta |
| Cal L R | : | California Law Review |
| Cr. L. J | : | Criminal Law Journal |
| Cr. P. C. | : | Code of Criminal Procedure |
| CoE | : | Council of Europe |
| Com | : | Committee |
| Del. | : | Delhi |
| Doc. | : | Document |
| DPAs | : | Data Protections Authorities |
| DPD | : | Data Protection Directive |
| e. g. | : | Example gratia (for Example) |
| Ed. | : | Edition |
| ECR | : | European Court Reports |
| ECHR | : | European Convention on Human Rights |
| E.H.R. R | : | European Human Rights Report |
| E.J.I. L | : | European Journal of International Law |

| | | |
|---|---|---|
| EP | : | European Parliament |
| EPW | : | Economic and Political Weekly |
| E. R | : | English Reports |
| EU | : | European Union |
| EWHC | : | High Court of England and Wales |
| FB | : | Full Bench |
| FDPC | : | Federal Data Protection Commission |
| GA | : | General Assembly of the United Nations |
| GDPR | : | General Data Protection Regulations |
| GPS | : | Global Position System |
| H.C | : | High Court |
| HR | : | Human Rights |
| HRC | : | Human Rights Committee |
| HRQ | : | Human Right Quarterly |
| H.R.L. J | : | Human Rights Law Journal |
| Harv. L. R | : | Harvard Law Review |
| I.A. | : | Indian Appeals |
| Ibid | : | In the same place (Ibidem) |
| IBA | : | International Bar Association |
| IBR | : | Indian Bar Review |
| IC | : | Indian Cases |
| ICCPR | : | International Covenant on Civil and Political Rights |
| ICESCR | : | International Covenant on Economic, Social and Cultural |
| ICJ | : | International court of Justice |
| ICLQ | : | International and Comparative Law Quarterly |
| ICR | : | Industrial Cases Reports |
| ICRC | : | International Committee of the Red Cross |
| I.E | : | Indian Express |
| i.e. | : | id est (that is) |
| IJIL | : | Indian Journal of International Law |

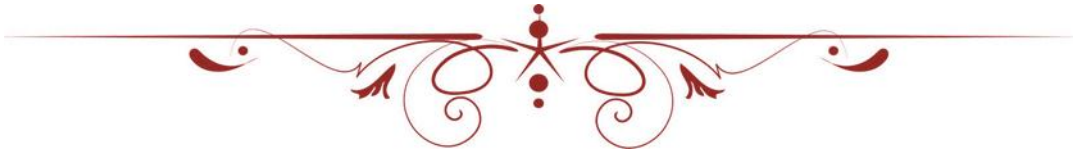
| | | |
|---|---|---|
| IJPA | : | Indian Journal of Parliamentary Affair |
| IJPA | : | Indian Journal of Public Administration |
| ILI | : | Indian Law Institute |
| ILO | : | International Labour Organizations |
| ILR | : | Indian Law Reports |
| Infra | : | Below |
| IPPs | : | Information Privacy Principles |
| IPC | : | Indian Penal Code |
| ITU | : | International Telecommunications Union |
| JBCI | : | Journal of Bar Council of India |
| JCPS | : | Journal of Constitutional and Parliamentary Studies |
| J. C. L& Crim. | : | Journal of Criminal Law and Criminology |
| JILI | : | Journal of Indian Law Institute |
| JT | : | Judgement Today (SC) |
| j. | : | Journal |
| KLT | : | Kerala Law Times |
| Lit. | : | Litigation |
| LQR | : | Law Quarterly Review |
| LT | : | Law Times |
| MP | : | Madhya Pradesh |
| MLJ | : | Madras Law Journal |
| MLR | : | Modern Law Review |
| NGO | : | Non-Governmental Organization |
| NHRC | : | National Human Rights Commission |
| N. Y | : | New York |
| N.Y.U. L. REV: | | New York University Law Review |
| N.Z.L. R | : | New Zealand Law Reports |
| OAS | : | Organization of African States |
| OAU | : | Organization of African Unity |
| OECD | : | Organization for Economic Corporation and Development |

| | | |
|---|---|---|
| O.J.L. S | : | Oxford Journal of Legal Studies |
| OSN | : | Online Social Network |
| OSNs | : | Online Social Networking Sites |
| P., PP. | : | Page; Pages |
| P.C | : | Privy Council |
| Para | : | Paragraph |
| PFI | : | Public Financial Institutions |
| PIL | : | Public Interest Litigation |
| PLT | : | Political and Law Times |
| Pt | : | Part |
| QB | : | Queen Bench |
| QBD | : | Queens Bench Division |
| RFID | : | Radio-frequency identification |
| RTI | : | Right to Information Act |
| Sec | : | Section |
| SC | : | Supreme Court |
| SCC | : | Supreme Court Cases |
| SCJ | : | Supreme Court Journal |
| SCR | : | Supreme Court Reports |
| SNSs | : | Social networking sites |
| Supp | : | Supplementary |
| Supra | : | Above |
| UDHR | : | Universal Declaration of Human Rights |
| UK | : | United Kingdom |
| UKHL | : | United Kingdom House of Lords |
| UN | : | United Nations |
| UNC | : | United Nations Charter |
| UNGA | : | United Nations General Assembly |
| UOI | : | Union of India |
| u/s | : | Under Section |

| | | |
|---|---|---|
| USA | : | United States of America |
| U.T.L. J | : | University of Toronto Law Journal |
| Vs. | : | versus |
| viz. | : | namely |
| Vol. | : | Volume |
| w.e.f. | : | With effect from |
| WHO | : | World Health Organization |
| WLR | : | Weekly Law Reports |
| WTO | : | World Trade Organization |
| Yale. L. J | : | Yale Law Journal |



# Chapter I
# Introduction



# Chapter I
# Introduction

## 1.1. 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 issues. 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[1].

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.[2]

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.

[1] Noriswadi Ismail and Edwin Lee Yong Cieh, et. at (eds.), *Beyond Data Protection* 6 (Springer, London, 2013)
[2] *Ibid.*

The processing of personal data has therefore become a key activity within the private and public sector.[3]

## 1.2. The concept of Privacy

The right to privacy was originally described as the 'right to be left alone' by the US Judge Thomas M. Cooley in 1888.[4] Shortly afterward, the concept of privacy was further articulated and made famous by two Harvard scholars, Warren and Brandeis, in their most celebrated and widely cited article, The Right to Privacy.[5]

The learned authors at that time had already recognized that, with the emergence of new technologies in printing press and photographs, the right to privacy had become a form of valuable social interest, which ought to be explicitly protected by the law.

The concept of privacy differs from one country to another. Due to the distinct concept of privacy, it has no universal definition. Privacy has been described as 'the interest that individuals have in sustaining a personal space, free from interference by other people and organization.[6] Professor Alan Westin argues that privacy is 'the claim of individuals to determine for themselves, when, how and to what extent information about themselves is communicated to others.[7] Privacy can therefore be said to involve the right to control one's personal information and the ability to determine when and how that information should be processed and used.

The concept of privacy law can further be divided into four main facets, namely data privacy (which concerns an individual's right and interest to control the processing of his personal data being held by another); physical privacy (which involves the protection of an individual from physical interference against his will); communications and surveillance privacy (which concerns an individual's right to have privacy protection from being monitored, be it in the form of surveillance or interception in communications), and territorial privacy (which involves the

[3] Supra note 1 at 1
[4] Cooley (1888), p. 29.
[5] Warren and Brandeis (1890).
[6] Clark (1997).
[7] Westin (1970), p. 7.

protection of an individual from having unlawful intrusion into his or her private space or workplace). This book is mainly concerned with the first facet i.e. data privacy, which is also referred to as data protection/information privacy.

Different jurisdictions may view data protection differently. Data protection is seen as a fundamental human right for individuals in Europe, while the US treats data protection as a private and consumer protection matter. Due to the differences in their perception towards data protection, it has been treated differently both in Europe and the US. In Europe, comprehensive data protection laws have been drawn up to protect their citizens' personal data. On the other hand, the US prefers a sectoral, self-regulatory approach to data protection, where a range of statutes have been enacted to regulate specific forms of data protection.

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.

## 1.3. Instrument for the protections of Data Privacy

### 1.3.1. International Level

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[8], and OECD Guidelines[9] EU Data Protection Directive[10], APEC Privacy Framework[11], 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.

[8] Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981
[9] Organisation for Economic Corporation and Development Guideline Governing the Protection of Privacy and Tran-Border Flows of Personal Data 1980
[10]European Community Directive on the Protection on the Individuals with Regards to the Processing of Personal Data and Free Movement of Such Data
[11] Asia Pacific Economic Corporation Privacy framework 2004

### 1.3.2. National Level

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***[12] 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.

Article 19(1) (a) stipulates that "all citizens shall have the right to freedom of speech and expression". However, this is qualified by Article 19(2) which states 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, decency or morality, or in relation to contempt of court, defamation or incitement to an offence". Thus, the freedom of expression guaranteed by Article 19(1) (a) is not absolute, but a qualified

[12] 2017(10) SCALE 1

right that is susceptible, under the Constitutional scheme, to being curtailed under specified conditions.

Article 21 reads "No person shall be deprived of his life or personal liberty except according to procedure established by law." Article 21 only requires a "procedure established by law" as a pre-condition for the deprivation of life and liberty.

Recently in case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[13] 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.

The movement towards the recognition of right to privacy in India started with ***Kharak Singh vs The State of U.P***.[14] 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.

[13] 2017(10) SCALE 1
[14] AIR 1963 SC 1295

In 1972, the Supreme Court decided a case one of the first of its kind on wiretapping. In ***R. M. Malkani vs State of Maharashtra***[15] 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***[16] 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***[17]**.** 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. The case related to the alleged autobiography of Auto Shankar who was convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various police 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

[15] AIR 1973 SC 157
[16] (1975)2 SCC 148
[17] (1994)6 SCC 632

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***[18] the court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right to privacy. The Supreme court held: 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.

Finally, Supreme Court of India in case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[19] 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.

Right to privacy granted under Article 21 of the Constitution of India, our jurisprudence, judicial pronouncements and case laws have extended it to encompass inter alia, a life of dignity. However, there is no express statutory grant of right to privacy and data protection.

### 1.4. New Approach for Data Protection in India

With the increased proliferation of technology in daily lives, it is becoming increasingly important for us to recognize and implement a meaningful right to privacy as also recognized by the Special Rapporteur on the Right to Privacy.

On one hand, there is significant success of Aadhaar, which is the largest biometric database in the world, as a means to implement social welfare schemes and

[18] AIR 1997 SC 568
[19] 2017(10) SCALE 1

serves as a tool for financial inclusion. On the other hand, there is reasonable apprehension as to the security of the information contained in the database and during any information transmission as a part thereof.

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.

The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy. Instrumentally, a firm legal framework for data protection is the foundation on which data driven innovation and entrepreneurship can flourish in India. Fostering such innovation and entrepreneurship is essential if India is to lead its citizens and the world into a digital future committed to empowerment, experiment and equal access.

In the case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[20] supreme court observed that,

[20] 2017(10) SCALE 1

*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 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.

Data protection is a big problem in India. So, it needs a specific Data Protection Law in India for present and future generations.

### 1.5. 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 of the data privacy matters. So, it requires 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.

### 1.6. Review of Literature

I have gone through the "The personal Data Protection Bill, 2014, The Right To Privacy Of Personal Data Bill, 2016, The Privacy (Protection) Bill, 2013, Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act-2016, The Data (Privacy And Protection) Bill, 2017, Information Technology Act, 2000 and also studied H.M. Seervai's "Constitutional Law of India", M.P. Jain's "Indian Constitutional Law", V.N. Shukla's "Constitution of India" Normann Witzleb and David Lindsay "Emerging Challenge in Privacy Law", Noriswadi Islami and Edwin Lee Yong Cieh "Beyond Data Protection". I also studied Articles "The Right to Privacy in the age of Information and Communications" by Madhavi Divan, "Aadhar Card- is it an intrusion into privacy? by Mrinal Sharma, "The Substantive Right to Privacy: Tracing the Doctrinal Shadows of the Indian Constitution" by Abhinav Chandrachud, "Right to Privacy in India""by Arjun Uppal and "Data Protection Laws in India" by Vijay Pal Dalmia "Data Protection in India: The Legislation of Self-Regulation" by Adrienne D'Luna Directo.

## 1.7. 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.

## 1.8. 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.

## 1.9. 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

## 1.10. 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"

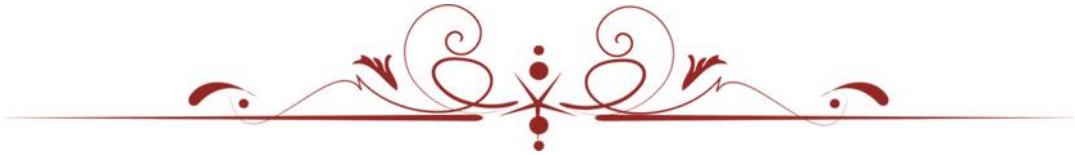
**Chapter V**- Judicial Travelling on the Issue of Privacy and Data Protection

**Chapter VI**- Reporting Research Findings

**Chapter VII**- Concluding Remarks

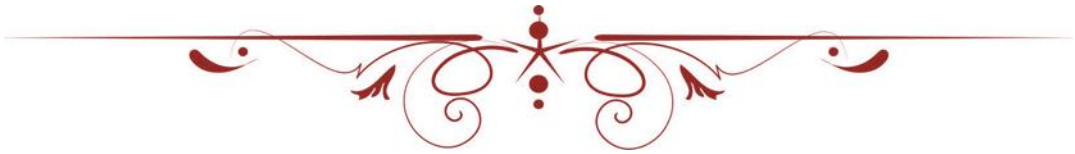
**Conclusion**

**Suggestions**



# Chapter II

# Right to Privacy and Data Protection



# Chapter II
# Right to Privacy and Data Protection

## Part A: International Perspectives -

### 2.1. Introduction

In the global information economy, personal data have become the fuel driving much of current online activity. Every day, vast amounts of information are transmitted, stored and collected across the globe, enabled by massive improvements in computing and communication power. In developing countries, online social, economic and financial activities have been facilitated through mobile phone uptake and greater Internet connectivity. As more and more economic and social activities move online, the importance of data protection and privacy is increasingly recognized, not least in the context of international trade. At the same time, the current system for data protection is highly fragmented, with diverging global, regional and national regulatory approaches.

The aetiology of data privacy law is complex. In a nutshell, data privacy result from an attempt to secure the privacy, autonomy and integrity of individuals and thereby the base for democratic, pluralist society in the face of massive growth in the amount of personal data gathered and shared by organizations.[21]

In developing and shaping data privacy law, the Council of Europe (CoE), Organization for Economic Cooperation and Development (OECD), United Nations (UN)and European Union (EU) have a long time played the main roles at the International level, although not always uniformly or concurrently.[22] A large range of other inter-governmental and non-governmental organization have played a relatively, though not insignificant, role in setting data privacy standards. These includes the World Trade Organization (WTO) International Labour Organizations (ILO) International Telecommunications Union (ITU). A particularly notable development

[21] Lee A. Bygrave Data Privacy Law: An International Perspective 8 (Oxford University Press, United Kingdom, 1st edn. 2014).
[22] Lee A. Bygrave Data Privacy Law: An International Perspective 18 (Oxford University Press, United Kingdom, 1st edn. 2014).

over the last decade is the emergence of organization in the Asia- Pacific and African region as policy brokers in the field. These include the Asia-Pacific Economic Cooperation (APEC).

### 2.2. Council of Europe

#### 2.2.1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

The Council of Europe was one of the first international bodies to begin developing normative response to the threats posed by computer technology to privacy related interest. It is the only international body to have draft a multilateral treaty dealing directly with data privacy.

It was the first legally binding international instrument in the data protection field. It was open for signature on 28 January 1981**.** A first step in this direction was taken in 1973 and 1974, with the adoption of Resolutions (73) 22 and (74) 29 which established principles for the protection of personal data in automated data banks in the private sector and the public sector. The objective was to set in motion the development of national legislation based on these resolutions.

In January 1981 the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[23] The Convention entered into force in October 1985. It is important to recognize that the Convention is a multilateral treaty as distinct from a statutory act of the Council of Europe. It is therefore legally binding under international law only upon those states that express consent to be bound through the formal act of ratification or accession. As of December 2003, thirty of the Council of Europe's forty-five member states were parties to the Convention and a further five had signed it. The Convention is also open to accession by non-member states of the Council of Europe but so far it has not attracted any non-member parties. The Convention was the first binding international instrument to protect individuals against abuses in the collection and processing of their personal data. It covers automated personal data files and automatic processing of personal data in the public and private sectors.

[23] available at http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (visited July 2, 2019)

**Purpose**

Its purpose is threefold:

**(1)** to introduce basic principles for fair information processing;
**(2)** to establish rules and restrictions on transborder data flows;
**(3)** to put into place mechanisms for consultation and mutual assistance between the parties.

The heat of the Convention lies in Chapter II which is broad-brush fashion, setout basic principal for Processing of personal data. It begins Article 4 with. Article 4 provided that,

It begins with an obligation on state parties to "take the necessary measures" to give effect to the basic principles for data protection in domestic law.[24] The term "necessary measures" is not defined and leaves the question of how to give effect to the rules to the discretion of the member states. The Explanatory Report to the Convention explains that apart from legislation, this requirement could also be met by the introduction of regulations or administrative guidelines. It continues that these binding measures could be supplemented by voluntary codes but makes clear that such codes alone would not suffice to comply with the Convention In practice, nearly all state parties have chosen to implement the Convention through legislation. The requirement in Article 4 is coupled with an "undertaking" in Article 10 to provide "appropriate sanction and remedies"[25] for violations of data protection principles as implemented into domestic law. Again, the Convention does not specify what constitutes "appropriate" sanctions and remedies. The Explanatory Report lists civil, administrative or criminal measures as possibilities.

The substantive principles of data protection are set out in Articles 5, 6, 7 and 8. Article 5, provides that all data undergoing automatic processing must be:

a) obtained and processed fairly and lawfully;

[24] Article 4 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[25] Article 10 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

d) accurate and, where necessary, kept up to date;

e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[26]

Article 6 Provided that

*"Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions"*[27].

Article 6 Explain the concept of special protection for "sensitive data" which is defined as data revealing racial origin, political opinions, religious or other beliefs, as well as data relating to health, sexual life or criminal convictions. Processing of these type of data is prohibited in the absence of appropriate legal safeguards. List of Sensitive Personal Data which is given in Article 6, are not exhaustive, it may be extended, in accordance with Article 11, to other kinds of data to take into account differing legal and sociological contexts.

Article 7 provided that,

*"Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination."*[28]

[26] Article 5 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[27] Article 6 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[28] Article 7 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.

Article 7 requires information processors to put into place appropriate security measures to protect against "accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

*"Any person shall be enabled:*

*a) To establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;*

*b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;*

*c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention*

*d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with*[29].

Article 8 implements the right of individuals to access information concerning them and to demand correction or erasure of this information if it has been processed in a manner inconsistent with the basic principles set out above.

Article 9 Provided that,

*"No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article*."[30]

[29] Article 8 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[30] Article 9 clause (1) of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.

According to clause (1) of Article 9 The principles set out in Articles 5, 6 and 8 are not absolute and may be departed from in accordance with one or more of the specific exemptions provided by Article 9.

Article 9 clause (2) provided that,

*"such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of,*

***a.*** *protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences*

***b****. protecting the data subject or the rights and freedoms of others"*[31].

This article provides that derogations of the principles are allowed where they are "provided for by the law of the Party" and "necessary measures in a democratic society" in order to protect "State security, public safety, the monetary interests of the State or the suppression of criminal offences" or to protect "the data subject or the rights and freedoms of others."

Article 9 clause (3) provided that,

*"Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects".*[32]

Article 9 clause (3) impose restrictions on "rights to access" provided in Article 8. Which are allowed "for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects."

Chapter III of this convention, concerned with the "Issue of transborder flows of data". It deals primarily with the transfer of personal information between parties to the Convention.

[31] Article 9 clause (2) of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[32] Article 9 clause (3) of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981

Article 12 clause (2) provided that,

*"A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party"*[33]

It takes as its point of departure the general rule that "a state party shall not, for the sole purpose of the protection of privacy, prohibit, or subject to special authorization transborder flows of personal data to the territory of another party."

Article 12 clause (3) (a) provided that,

*"Insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection"*[34]

Its permits state parties to derogate from this general rule and to prohibit transfers of certain categories of personal data or of automated personal data files which are specifically protected in its national laws and for which the receiving party does not provide "equivalent protection."

According to Article 12 clause (3) (b), It also permits parties to prohibit transfers to other contracting parties if the data is destined for a non-contracting party in circumvention of the first party's national law. This provision is intended to prevent data being "laundered" through the intermediary of another state party on its way to a non-contracting state which does not have a satisfactory data protection regime.[35]

The Convention itself does not deal with the direct transfer of data to non-contracting parties leaving the matter up to the national laws of state parties. This issue is now addressed in the Additional Protocol.

[33] Article 12 clause (2) of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[34] Article 12 clause (2) of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[35] Article 12 clause (3) (b) of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.

Chapters IV and V provide a mechanism for implementation and oversight of the Convention. Article 13 of this convention imposes a duty to parties, to designate an authority for purposes of co-operation with and assistance to other parties.[36]

Article 14 concerns assistance to data subjects residing abroad who wish to exercise their rights of access under Article 8. It stipulates that data subjects residing in another contracting state are to be given the option of using that country's designated authority as an intermediary in order to exercise their access rights.[37]

Chapter V dealt the provision related to the Consultative Committee. Articles 18-20 dealt the establish a "Consultative Committee"[38] to be made up of a representative and deputy representative of each contracting party. Non-contracting member states are entitled to observer status on the Committee. Committee is not given any enforcement powers. Its main functions are to propose ways to facilitate or improve the application of the Convention and to make proposals for its amendment.[39] It is to meet at least once every two years or when one-third of the representatives of the parties request it to do so.[40]

### 2.2.2. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001

In November 2001, the Council of Europe adopted an Additional Protocol to its 1981 Data Protection Convention.

The Protocol is intended to close two major shortcomings of the Convention

(1) Failure to address transborder data flows to non-contracting states, and
(2) Failure to establish national supervisory bodies.

[36] Article 13 of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[37] Article 14 of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981.
[38] Article 18 of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981
[39] Article 19 of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981
[40] Article 20 of "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data1981

It is a short instrument containing only two substantive provisions.

(1) Article 1 requires parties to establish independent supervisory authorities to ensure compliance with the principles of the Convention and the Protocol.[41]

(2) Article 2 requires parties to prohibit transfers of personal data to non-contracting states that do not provide an "adequate level of protection for the intended data transfer.[42]

Article 1 provided that; provision related to "Supervisory Authorities"

Article 1 clause (2) (a) provided that,

*"…….authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities' violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol."*[43]

and Article 1 clause (2) (b) provided that,

"*Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence*"[44]

According to Article 1 clause (2) (a) and clause (2) (b),

These authorities are to be granted the power to receive complaints, to investigate and intervene in cases, to engage in legal proceedings and to refer violations to competent judicial authorities.

According to Article 1 clause (4), Parties have right to appeal, to the court against the decisions of the supervisory authorities.[45]

---

[41] Article 1 of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (2001)

[42] Article 2 of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (2001)

[43] Article 1 Clause (2)(a) of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (2001)

[44] Article 1 Clause (2)(b) of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (2001)

According to Article 1 clause (5), Supervisory authorities are to "co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging useful information."[46]

According to the Explanatory Report to the Protocol,

Article 1 has a dual aim:

(1) to enforce the effective protection of the individual; and
(2) to improve harmonization of the rules governing the supervisory authorities already established by parties to the Convention.[47]

The Report also clarifies that the powers listed in Article 1 are not intended to be exhaustive and that supervisory authorities may also be entitled to carryout additional duties such as prior checks on processing operations; the maintenance of a public register of data processors; and commentary on proposed legislative, regulatory or administrative measures relating to data processing. Article 2 requires parties to prohibit transfers of personal data to non-contracting states that do not provide an "adequate level of protection for the intended data transfer." Exceptions to this general rule may be provided by law for the "specific interests of the data subject;" or "legitimate prevailing interests, especially important public interests;" or where safeguards are put in place by the controller, for example on the basis of contractual clauses, and these safeguards are deemed adequate by the competent authorities.

The Explanatory Report notes that the "adequacy" of the level of protection must be assessed in light of all the circumstances relating to the transfer including the type of data, the purpose and duration of processing, the country of origin and final destination, and the laws applicable in the state or organization. Furthermore, regard must be had to the principles of Chapter II of the Convention and their implementation in the recipient state or organization. Adequacy can be assessed on a case-by-case basis or for a whole state or organization. At the request of one of the

[45] Article 1 Clause (4) of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (2001)
[46] Article 1 Clause (5) of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (2001)
[47] Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 181),

parties, the Consultative Committee may issue an opinion on the level of protection in a state or organization.

With respect to derogations, the Explanatory Report states that parties must "respect the principle inherent in European law that clauses making exceptions are interpreted restrictively, so that the exception does not become the rule." As examples of "legitimate prevailing interests" it refers to the public interests set out in Article 8(2) of the European Convention on Human Rights and in Article 9(2) of the 1981 Convention; the exercise or Defence of a legal claim; or the extraction of data from a public register. As an example of the "specific interests of the data subject" it gives the fulfilment of a contract with, or on behalf of the data subject. It also notes that exceptions may be allowed where the data subject has given his or her consent, provided it is given on the basis of appropriate information. Where safeguards are put in place as a result of contractual clauses, the Report stipulates that the content of the contract must include all relevant elements of data protection. Furthermore, it suggests inclusion of procedural terms such as naming a contact person within the staff of the transferring body who would be responsible for ensuring compliance and whom the data subject would be free to contact.

### 2.3. European Union Initiatives

#### 2.3.1. EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data 1995

The institutional organs of the EU and its predecessors (the European Economic Community and European Community) were slower off the mark than their counterparts in the CoE, OECD, and UN to develop data privacy instruments. The EU instrument was most ambitious comprehensive, and complex in the field. The central instrument is the Data Protection Directive (DPD).[48] Since its adoption in October1995, it has constituted the most important point of departure for national data privacy initiatives within and to a large extent, outside the EU.[49]

[48] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995

[49] Lee A. Bygrave, Data Privacy Law: An International Perspective 53 (Oxford University Press, United Kingdom, 1st edn. 2014).

The adoption of the DPD is the culmination of a series of proposal, strung over two decades, urging EU member state to take legal action in the field of data privacy. Initially most active institutional actor in this context was the European Parliament (EP). It concerns to protect human rights in the face of developments in the computer technology. The European Commission, along with the Council of Ministers, was considerably more reserved in taking up the issue.[50]

During the 1970s the European Parliament conducted extensive studies in the area of data protection. Concerned that differences in national laws on data protection could result in obstacles to the functioning of a European common market, the Parliament repeatedly recommended the introduction of a directive in this area.

The first major initiative taken by the Commission with respect to data privacy was to issue a Recommendation in 1981echoing calls by the Parliament for member state to sing and ratify Convention 108.[51] Towards the end of the 1980s, the commission began work on drafting a framework Directive on data privacy. The commission issued its first proposal for a framework Directive on data privacy in 1990.[52] Accompanying this initiative were, inter alia a proposal for a more specialized Directive on data privacy in the context of telecommunications,[53] and a proposal on information security measures.[54]

By the 1990s, it was clear that the Convention was not realizing its goal of harmonization of national laws on data protection. Although a number of European countries had introduced data protection laws based on the Convention, there were often considerable differences in the provisions of these laws.

The 1990 proposal for a framework Directive on data privacy was met with much criticism. The Commission issued an amended proposal in 1992 after extensive input from the European Parliament.

---

[50] Lee A. Bygrave Data Privacy Law: An International Perspective 54 (Oxford University Press, United Kingdom, 1st edn. 2014).

[51] Lee A. Bygrave Data Privacy Law: An International Perspective 55 (Oxford University Press, United Kingdom, 1st edn. 2014).

[52] See Proposal for a Council Directive Concerning the protection of individuals in relations to the processing of personal data (1990) OJ C277/3

[53] See Proposal for a Council Directive Concerning the protection of personal data and privacy in the context of public digital telecommunications network, in particular the integrated service digital network (ISDN)and public mobile digital networks (1990) OJ C277/12

[54] See Proposal for s Council Decision in the field of information Security (1992) OJ L123/19

The 1990s draft directive was revised and redrafted a number of times as it made its way through each of the different institutions of the European Community. Finally, in 1995 the Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data was approved. The Directive seeks to harmonize national laws within the European Union in order to facilitate the free flow of information across the internal market while simultaneously ensuring a high level of privacy protection for individuals. The European Directive is the most detailed and complex of the international data protection instruments.[55]

Unlike the 1981 Council of Europe Convention which applies only to automated processing of personal data, the Directive applies to "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form a part of a filing system."[56] However, its scope is limited in two major respects. Although, the Directive generally applies to processing in both the private sectors, it does not apply to the processing of personal data in the course of activities falling outside the scope of Community law.

### 2.3.2. Interpretation of DPD

Interpreting the DPD is no easy task. Chapter I of DPD provided general provision related to the data protection. Article 1 provide the "Object of the Directive". Fallowing objective are given in the DPD.

(1) *"In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."*

(2) *"Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1"*

According to Article 1 it is the duty of the member state to protect the fundamental right and freedom of natural person in respect of data privacy. It is the

[55] Lee A. Bygrave Data Privacy Law: An International Perspective 56 (Oxford University Press, United Kingdom, 1st edn. 2014).
[56] Art. 3 clause (1) EU Directive, 1995.

duty of member state to nor prohibit the free flow of personal data between member state.

Article 3 provided that the scope of the DPD. DPD is apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data.

However, its scope is limited in two major respects. Although, the Directive generally applies to processing in both the private sectors, it does not apply to the processing of personal data in the course of activities falling outside the scope of Community law. This includes processing concerning public security, Defence, State security, and the activities of the State in areas of criminal law. Second, it does not apply to processing by a natural person in the course of "a purely personal or household activity."[57]

Chapter II sets out the "General Rules on the Lawfulness of the Processing of Personal Data". It reiterates the principles of the 1981 Council of Europe Convention and extends the protections of that instrument by creating new rights for individuals.

Chapter II set out the basic principles of fair Data Processing. Article 6 provides that personal data must be:

**1)** Processed fairly and lawfully;

**2)** Collected for specified, explicit and legitimate purposes and not others

**3)** Processed in a way incompatible with those purposes.

**4)** Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

**5)** Accurate, kept up to date, erased or rectified;

**6)** Kept in a form which permits identification of data subjects for no longer than is necessary.[58]

[57] Art. 3 clause (2) EU Directive, 1995.
[58] Article 6, EU Directive, 1995.

Article 7 provided that "Criteria for Making Data Processing Legitimate". Article 7 provides that processing may only take place if the data subject has "unambiguously" given consent or if processing is necessary

**1)** for the performance of a contract to which the data subject is a party

**2)** for compliance with a legal obligation

**3)** in order to protect the vital interests of the data subject

**4)** for the performance of a task carried out in the public interest or in the exercise of official authority

**5)** for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.[59]

Data Protection Directive provides extra protections for "sensitive" data. which is provided in Article 8. According to Article 8 Personal Data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing of this data is prohibited except where the data subject has given "explicit" consent or where the processing is

**1)** Necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent[60]

**2)** Necessary for carrying out the controller's obligations in the area of Employment Law[61]

**3)** Necessary for the establishment, exercise, or defense of a legal claim relates to data which are manifestly made public by the data subject[62]

**4)** Carried out a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim in the course of the legitimate

[59] Article 7, EU Directive, 1995.
[60] Article 8 clause (2)(c) of the European Union Data Protection Directive, 1995.
[61] Article 8 clause (2)(b) of the European Union Data Protection Directive, 1995.
[62] Article 8 clause (2)(e) of the European Union Data Protection Directive, 1995.

activities and where it relates solely to the members of the body and is not disclosed to a third party.[63]

Article 9 provided provision related to "Processing of personal data and freedom of expression". According to Article 9 it is the duty of member state to provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data. Exemptions or derogations from the provision on fallowing purpose

**(1)** journalistic
**(2)** artistic or
**(3)** literary expression

if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[64]

Articles 10 to 15 provided a series of rights to data subjects. Articles 10 and 11 provide that "Right to know". These articles are stipulate that data subjects are to be provided with information concerning

**(1)** Identity of data controllers and of his representative,[65]
**(2)** Purposes of the data processing[66]
**(3)** Recipients of the data[67]
**(4)** Existence of a right to access and rectify data.[68]

Article 12 provide that the "Right to Access". In this article data subjects are entitled to obtain "without constraint at reasonable intervals and without excessive delay or cost"

**(1)** Confirmation of whether personal data is being processed
**(2)** details to its intended purpose and use
**(3)** Information, which are the logic involved in any automatic processing of data[69].

[63] Article 8 clause (2)(d) of the European Union Data Protection Directive, 1995.
[64] Article 9 of the European Union Data Protection Directive, 1995.
[65] Article 11 clause (1)(a) of the European Union Data Protection Directive, 1995.
[66] Article 11 clause (1)(b) of the European Union Data Protection Directive, 1995.
[67] Article 11 clause (2)(d) of the European Union Data Protection Directive, 1995.
[68] Ibid.

Data subjects have right to the rectification, erasure or blocking of processing of data, which are inaccurate or incomplete or violates the provisions of the Directive.[70]

Where it's possible and not involving a disproportionate effort, controllers are to notify third parties to whom data has been disclosed of any such rectification, erasure or blocking of processing.[71]

Article 14 provide that's "The data subject's right to object". Data Subjects have right to object at any time on legitimate grounds to processing being carried out for certain purposes, including direct marketing.[72]

Article 15 establishes the right of individuals not to be subject to decisions made solely on the basis of automated data processing. Provided that suitable safeguards are in place exceptions to this right are permitted for decisions taken in the course of entering into or performance of a contract, or for decisions authorized by law.[73]

Articles 16 to 19 concern the duties of data controllers. Article 16 provide that, obligation of Data Controller in respect to the confidentiality of processing,[74] to ensure a "high level of security appropriate to the risks represented by the processing and the nature of the data;"[75] and to notify the supervisory authority whenever its processing operations are to be wholly or partly automated.[76]

Chapter III of the Data Protection Directive Provide Provision related to judicial remedies, liability and sanctions. Article 22 provide the provision related to judicial remedy.

"…*Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question".*[77]

---

[69] Article 12 clause (1)(a) of the European Union Data Protection Directive, 1995.
[70] Article 12 clause (1)(b) of the European Union Data Protection Directive, 1995.
[71] Article 12 clause (1)(c) of the European Union Data Protection Directive, 1995.
[72] Article 14 of the European Union Data Protection Directive, 1995.
[73] Article 15 of the European Union Data Protection Directive, 1995.
[74] Article 16 of the European Union Data Protection Directive, 1995.
[75] Article 17 of the European Union Data Protection Directive, 1995.
[76] *Ibid.*
[77] Article 22 of the European Union Data Protection Directive, 1995.

According to this Article, member states to provide judicial remedy for breaches of their rights to the individuals.

Article 23 provide that Lability of data controller for processing of personal data.

*"... any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered"*[78]

Article 23 impose liability on data controllers to provide compensation to data subjects for damage caused by unlawful processing. Article 24 provide provision related to sanctions for infringements of the Data Protection Directive.[79]

Chapter IV provide provisions related to "Transborder flows of personal data to the third country. Article 25 provide provision related to general principles of data transfers to third country and country ensures an adequate level of protection. The question of adequacy is to be assessed "in light of all the circumstances surrounding the transfer including the

**(1)** Nature of the data,
**(2)** Purpose and proposed duration of the processing;
**(3)** Country of origin and final destination of data
**(4)** Laws, professional rules, and security measures in place in the third country.[80]

Where the Commission finds that a third country does not ensure an "adequate level of protection," member states are required to take "all measures necessary" to block transfers to that country.[81]

Article 26 provide provision related to derogations from the Article 25. Article 26 provide exceptions, on the fallowing grounds,

**(1)** when the data subject has given "unambiguous" consent,

[78] Article 23 of the European Union Data Protection Directive, 1995.
[79] Article 24 of the European Union Data Protection Directive, 1995.
[80] Article 25 clause (2) of the European Union Data Protection Directive, 1995.
[81] Article 25 clause (4) of the European Union Data Protection Directive, 1995.

**(2)** when the data to be transferred is already contained in a public register,

**(3)** when the transfer is necessary for the

**a)** Performance of a contract to which the data subject is a party

**b)** Importance for public interest grounds or for the establishment, exercise, or defense of legal claims

**c)** Protect the vital interests of the data subject[82]

Chapter VI provide the provision related to mechanisms for supervision and enforcement of the Data Protection Directive. Article 28 provide that each member state to establish one or more supervisory authorities to oversee application of the Directive[83]. These authorities must act "incomplete independence" and are to be in entrusted with a large number of powers and responsibilities.[84] Authority have power to to be consulted during the drafting of administrative measures or regulations concerning data protection.[85] They must also be empowered to monitor, investigate and intervene in data processing activities,[86] to hear complaints[87]; and to initiate legal proceedings.[88] In terms of responsibilities, supervisory authorities are to be required to issue annual reports and to maintain a public register containing information on data controllers operating wholly or partly automatic processing systems.[89]

Finally, Articles 29 and 30 provide provisions for the stablish Working Party. Its composed for the Protection of Individuals with regard to the Processing of Personal Data. It shall have advisory status and act independently.[90] Its representative of the supervisory authority of each member state, a representative of the Commission, and representative of other Community institutions.[91] The Working Party is empowered to issue advisory opinions on issues such as the uniform application of national measures to implement the Directive,[92] the level of protection

[82] Article 26 clause (1) of the European Union Data Protection Directive, 1995
[83] Article 28 clause (1) of the European Union Data Protection Directive, 1995
[84] *Ibid.*
[85] Article 28 clause (2) of the European Union Data Protection Directive, 1995
[86] Article 28 clause (3) of the European Union Data Protection Directive, 1995
[87] Article 28 clause (4) of the European Union Data Protection Directive, 1995
[88] Supra. note 53
[89] Article 28 clause (5) of the European Union Data Protection Directive, 1995
[90] Article 29 clause (1) of the European Union Data Protection Directive, 1995
[91] Article 29 clause (2) of the European Union Data Protection Directive, 1995
[92] Article 30 clause (1) of the European Union Data Protection Directive, 1995

in the Community and in third countries,[93] proposed amendments to the Directive,[94] and codes of conduct drawn up at the Community level.[95]

Finally, the Working Party is also entitled to issue recommendations on all matter relating to data protection and is required to issue an annual report regarding the level of protection for personal data within the Community and in third countries.[96]

### 2.4. OECD Initiative

The OECD began taking an interest in data privacy not long after the Council of Europe (CoE). In the early 1970s, it commissioned a number of reports on the issue as part of a series of Informatics Studies'. Later in that decade, it began work on drafting its own regulatory instrument. The Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data was adopted by the OECD Council on 23 September 1980 ("1980 Guidelines"). The 1980 Guidelines were adopted to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. The core of 1980 Guidelines is, set of eight data privacy principles. These core Principles apply to manual and electronic processing of personal data in both the public and private sectors.

The Guidelines are not legally binding on OECD member states. Their publication was simply accompanied by an OECD Council Recommendation stating that account should be taken of them when member countries develop domestic legislation on privacy and data protection.[52] The recommendation also stressed that member countries should endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to trans-border data flows of personal data.

#### 2.4.1. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data,

1980s Guidelines have provided general guidance of handling of personal information in the public and private sector. The guidelines:

[93] Article 30 clause (1)(b) of the European Union Data Protection Directive, 1995
[94] Article 30 clause (1)(c) of the European Union Data Protection Directive, 1995
[95] Article 30 clause (1)(d) of the European Union Data Protection Directive, 1995
[96] Article 30 clause (3) of the European Union Data Protection Directive, 1995

- Represent an international consensus on how best to balance effective privacy protection with the free flow of personal data.
- Are technology- neutral, flexible, allow for various means of compliance, and apply in all environments, including on global networks
- Have been put to use in a large number of national regulatory and self-regulatory instruments and are still widely used in both the public and private sector.

Part II of the Guideline provided Core Principles related to the data privacy. Para 7 provided "Collection Limitation Principle"[97]. According to this principle data collection should be 'with the knowledge and consent of the data subject.' Para 8 provided 'Data Quality Principle'[98]. According to this Personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete and kept up-to-date. Para 9 provided 'Purpose Specification Principle'. According to this Principle, the purpose for which personal data are collected should be specified not latter than at the time of data collection.[99] Para 10 provided 'Use Limitations Principles'. According to this principle, Personal data should not be disclosed, made available or otherwise used. It should be disclosed, made available or otherwise used with the consent of the data subject or by the authority of law.[100] Para 11 provide 'Security Safeguards Principle'. According to this para Personal data should be protected by reasonable security safeguards against any risks, loss or unauthorized access, destruction, use, modification or disclosure of data.[101] Para 12 provided 'Openness Principle'[102]. According to this principle data subject should be able to avail themselves of data collection and be able to contact the entity collecting this information. Para 13 provided 'Individual Participation Principle'[103]. According to this principle, Individual have right to obtain information related their personal data

[97] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 7 (adopted 23 September 1980; (C(80)58/FINAL).
[98] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 8 (adopted 23 September 1980; (C(80)58/FINAL).
[99] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 9 (adopted 23 September 1980; (C(80)58/FINAL).
[100] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 10 (adopted 23 September 1980; (C(80)58/FINAL).
[101] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 11 (adopted 23 September 1980; (C(80)58/FINAL).
[102] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 12 (adopted 23 September 1980; (C(80)58/FINAL).
[103] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 13 (adopted 23 September 1980; (C(80)58/FINAL).

within a reasonable time in reasonable manner. Para 14 provided 'Accountability Principle'[104]. This principle stipulates that, data controller should be accountable for comply with measure which give effect to the other all core principles which is related to data protection.[105]

Part third of the guideline dealt the "Basic principles of international application: free flow and legitimate restrictions"[106]. This part stipulated that it is the duty of member country to take all reasonable and appropriate steps to ensure that transborder flows of personal data. Part fourth of the guideline dealt the "National implementation"[107]. This part stipulated that it is the duty of members country, when he stablished any legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data, should fallow the Part second and part third principles.

### 2.4.2. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, (2013)

1980's Guidelines were revised and issued in a new version in September 2013. they were updated on 11 July 2013 due to changes in personal data usage, as well as new approaches to privacy protection. The Recommendation aims to promote and protect the fundamental values of privacy, individual liberties and the global free flow of information to foster the development of economic and social relations among Adherents. In this regards it addressed the consumer protection and empowerment, privacy and security in light of changing technologies, markets and user behaviors and the growing importance of digital identities.[108] The principle changes introduced by the revised Guidelines concern implementation and enforcement mechanisms. The

[104] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 14 (adopted 23 September 1980; (C(80)58/FINAL)
[105] Lee A. Bygrave Data Privacy Law: An International Perspective 48 (Oxford University Press, United Kingdom, 1st edn. 2014).
[106] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 15 -18 (adopted 23 September 1980; (C(80)58/FINAL)
[107] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 19 (adopted 23 September 1980; (C(80)58/FINAL)
[108] Lee A. Bygrave Data Privacy Law: An International Perspective 44 (Oxford University Press, United Kingdom, 1st edn. 2014).

Guidelines' legal status remains otherwise unchanged. Eight core principles are remained unchanged and, to a large extent, their rationale.[109]

Original Guidelines which pronounces a determination 'to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them'. This determination is repeated word for word in the Council Recommendation accompanying the revised Guidelines.

Part 3 of the Guidelines contains provisions on 'implementing accountability. These provisions were introduced in the 2013 revision. Its elaborate the accountability principle in paragraph 14 which stipulates that data controllers 'should be accountable for complying with | measures which give effect to the other Part 2 principles.[110] The key elements of the new Part 3 provisions are the need for a controller to draw up a 'privacy management programme' that provides for appropriate safeguards based on privacy risk assessment'.[111] Another central element Is a requirement for security breach notification. This means that a controller should provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data, notification should also extend to those data subjects who are 'likely' to be adversely affected by the breach.[112]

Part 4 deals specifically with regulating the flow of personal data across national borders. The rules here were modified in the 2013 revision but retain much the same approach as the original Guidelines. They begin with a re-elaboration of the accountability principle in the context of transborder data flow.[113] A data controller remains accountable for personal data under its control without regard to the location

[109] *Ibid.*
[110] Lee A. Bygrave Data Privacy Law: An International Perspective 48 (Oxford University Press, United Kingdom, 1st edn. 2014).
[111] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 15(a)(iii) (adopted 11 July 2013; (C (2013)79).
[112] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 15(c) (adopted 11 July 2013; (C (2013)79).
[113] Lee A. Bygrave Data Privacy Law: An International Perspective 48 (Oxford University Press, United Kingdom, 1st edn. 2014).

of the data.[114] The central rules are laid down in paragraphs 17 and 18**.** According to paragraph 17

"*A Member country should refrain from restricting transborder flows of personal data between itself and another country where*

***(a)*** *the other country substantially observes these Guidelines or*

***(b)*** *sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines*."[115]

An important difference between this and the previous version of paragraph 17 is that the latter dealt primarily with data flow between OECD member states, the new version is of more general application. Another important difference concerns the criteria for permitting restrictions on transborder data flow. The previous version of paragraph 17 permitted a member country to restrict such flow 'where the re-export of such data would circumvent its domestic privacy legislation'[116] or 'where the restrictions concerned certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection'[117]. The new version dispenses with these criteria.

Parts **5** and **6** of the Guidelines deal with their implementation and international cooperative efforts to advance their aims. Particularly noteworthy with these provisions is that they now recommend member countries to establish privacy enforcement authorities.[118]

---

[114] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 16 (adopted 11 July 2013; (C (2013)79).
[115] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 17 (adopted 11 July 2013; (C (2013)79).
[116] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 17 (adopted 23 September 1980; (C(80)58/FINAL)
[117] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 17 (adopted 23 September 1980; (C(80)58/FINAL)
[118] Lee A. Bygrave, Data Privacy Law: An International Perspective 49 (Oxford University Press, United Kingdom, 1st edn. 2014).

*"Establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis."*[119]

'Privacy enforcement authorities' embrace not just traditional DPAs but also other regulators with a role in enforcing data privacy law. Such authorities should be invested 'with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis.[120]

The Guidelines encouragement of 'self-regulation' whether in the form of codes of conduct or otherwise.[121] It's the obligations of members country to adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy.[122]

Further, the Guidelines exhort member countries 'to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing Information sharing among privacy enforcement authorities.[123]

## 2.5. APEC Initiatives

In 2003, the 21 member states of the Asia-Pacific Economic Cooperation formally began work on drafting a set of common principles to guide their respective regulatory approaches in the field. In November 2004, Ministers for the twenty-one APEC Economies endorsed the "APEC Privacy Framework". The Framework is comprised of a set of nine guiding principles and guidance on implementation to assist APEC Economies in developing consistent domestic approaches to personal information privacy protections. It also forms the basis for the development of a

[119] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 19(c) (adopted 11 July 2013; (C (2013)79).
[120] Supra note 86.
[121] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 19(d) (adopted 11 July 2013; (C (2013)79).
[122] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, para 19(g) (adopted 11 July 2013; (C (2013)79).
[123] Lee A. Bygrave, Data Privacy Law: An International Perspective 50 (Oxford University Press, United Kingdom, 1st edn. 2014).

regional approach to promote accountable and responsible transfers of personal information between APEC Economies.

The Framework is inspired by, and modelled upon, the OECD Guidelines rather than EU and CoE instruments. APEC Privacy Framework updated in 2015.

This Privacy Framework provides "a principles-based … framework as an important tool in encouraging the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region."[124]

APEC plays a critical role in the Asia Pacific region by promoting a policy framework designed to ensure the continued free flow of personal information across borders while establishing meaningful protection for the privacy and security of personal information.

### 2.5.1. Purpose of the framework

Purposes of the framework are to:[125]

- Develop appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information.
- Enable global organizations that collect, access, use or process data in APEC Economies to develop and implement uniform approaches within their organizations for global access to and use of personal information.
- Assist enforcement agencies in fulfilling their mandate to protect information privacy.
- Advance international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

Part I of this framework dealt the Preamble of the framework. Part II of this framework dealt the 'Scope'[126] of the framework. The purpose of Part II of the APEC

[124] APEC Privacy Framework, Part I, Preamble, para 4, 2015
[125] APEC Privacy Framework, Part I, Preamble, para 8, 2015
[126] APEC Privacy Framework, Part II, Scope, para 9 - 18, 2015

Privacy Framework is to make clear the extent of coverage of the Principles.[127] In this part given some important definition related to data protection. In this part define "Personal information"[128], "Personal information controller"[129], "Privacy Law"[130], "Privacy Enforcement Authority"[131] etc.

Part III is the heart of the framework. It is set of "Information Privacy Principles"[132] (IPPs). This Principles are mostly based on the core principles of the OECD Guidelines.

Part IV[133] of the framework, provided guidance to members for implementing the APEC Privacy Framework. It is divided in two section, Section A focuses on those measures' members should consider in implementing the Framework domestically, while Section B sets out APEC-wide arrangements for the implementation of the Framework's cross-border elements.[134]

Part A provided obligations to the members; they should have regard to the following basic concept in considering the adoption of measures designed for domestic implementation of the APEC Privacy Framework:[135]

- Maximizing Benefits of Privacy Protections and Information Flows[136]
- Giving Effect to the APEC Privacy Framework[137]
- Privacy Management Programme[138]
- Promotion of technical measures to protect privacy[139]
- Public education and communication[140]
- Cooperation within and between the Public and Private Sectors[141]

[127] APEC Privacy Framework, Part II, Scope, para 9 - 18, 2015
[128] APEC Privacy Framework, Part II, Scope, para 9, 2015
[129] APEC Privacy Framework, Part II, Scope, para 10, 2015
[130] APEC Privacy Framework, Part II, Scope, para 15, 2015
[131] APEC Privacy Framework, Part II, Scope, para 14, 2015
[132] APEC Privacy Framework, Part III, Information Privacy Principles, para19 - 32, 2015
[133] APEC Privacy Framework, Part IV, Implementation, para 33-72, 2015
[134] APEC Privacy Framework, Part IV, Implementation, para 33, 2015
[135] APEC Privacy Framework, Part IV, Implementation, para 34, 2015
[136] APEC Privacy Framework, Part IV, Implementation, para 35-36, 2015
[137] APEC Privacy Framework, Part IV, Implementation, para 37-42, 2015
[138] APEC Privacy Framework, Part IV, Implementation, para 43-45, 2015
[139] APEC Privacy Framework, Part IV, Implementation, para 46-47, 2015
[140] APEC Privacy Framework, Part IV, Implementation, para 48, 2015
[141] APEC Privacy Framework, Part IV, Implementation, para 49- 52, 2015

- Providing for appropriate remedies in situations where privacy protections are violated[142]
- Mechanism for Reporting Domestic Implementation of the APEC Privacy Framework[143]

Part B provided guidance for international implementation. In this regards it addressing the international implementation of the APEC Privacy Framework, and consistent with the provisions of Part A. It is the duty of members should consider the following points relating to the protection of the privacy of personal information:[144]

- Information sharing among member economies[145]
- Cross-border cooperation in investigation and enforcement[146]
- Cross-border privacy mechanisms[147]
- Cross-border transfers[148]
- Interoperability between privacy frameworks[149]

Subsequent to the Framework's adoption, APEC has put effort into facilitating cross-border flow of personal data in conformity for Accountability Principle. The effort was formalized in September 2007 as the 'Data Privacy Pathfinder'. Its first palpable result is the establishment of a Cross-Border Privacy Enforcement Arrangement (CPEA) in July 2010. This is a mechanism for the regions DPs to share information and assist each other in cross-border enforcement of data privacy rules. A second result is the endorsement of a Cross-Border Privacy Rules (CBPR) system in November 2011. This is a voluntary certification scheme whereby an organization may choose to develop internal policies governing transborder flow of personal data.[150]

[142] APEC Privacy Framework, Part IV, Implementation, para 53-54, 2015
[143] APEC Privacy Framework, Part IV, Implementation, para 55, 2015
[144] APEC Privacy Framework, Part IV, Implementation, para 56, 2015
[145] APEC Privacy Framework, Part IV, Implementation, para 57-61, 2015
[146] APEC Privacy Framework, Part IV, Implementation, para 62-64, 2015
[147] APEC Privacy Framework, Part IV, Implementation, para 65-68, 2015
[148] APEC Privacy Framework, Part IV, Implementation, para 69-70, 2015
[149] APEC Privacy Framework, Part IV, Implementation, para 71 - 72, 2015
[150] Lee A. Bygrave, Data Privacy Law: An International Perspective 78 (Oxford University Press, United Kingdom, 1st edn. 2014).

## 2.6. Human rights treaties

For the data privacy, Major human rights treaties, most notably the 1966 International Covenant on Civil and Political Rights (ICCPR)[151] and the ECHR, are now commonly seen as providing the central normative roots for data privacy law, and they are increasingly used as data privacy instruments in themselves. Jurisprudence developed pursuant to the right to privacy in ICCPR Article 17 and ECHR Article 8 provides the backbone for this development. Both sets of provisions have been authoritatively construed as requiring national implementation of the basic principles of data privacy laws.[152]

The operationalization of the human rights dimension of data privacy law is, however, far from uniform. It is much more developed in Western Europe than the Asia-Pacific. As, the APEC Privacy Framework shows scant regard for the connection between data privacy and human rights, while the ASEAN push for harmonized data privacy regimes is driven primarily by economic concerns.[153]

### 2.6.1. ICCPR Article 17

The UN Human Rights Committee was the first to clearly recognize that the right to privacy in ICCPR Article 17 provides certain data privacy guarantees. Article 17 states:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.*
2. *Everyone has the right to the protection of the law against such interference or attacks.*[154]

Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as

[151] UN General Assembly resolution 2200A (XXI) of December 16, 1966
[152] Lee A. Bygrave, Data Privacy Law: An International Perspective 82-83 (Oxford University Press, United Kingdom, 1st edn. 2014).
[153] Ibid, page 83
[154] Article 14 of the **International Covenant on Civil and Political Rights (ICCPR**) 1966.

against unlawful attacks on his honour and reputation.[155] This right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons.[156] According to this article it is the obligations on State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[157]

The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.[158]

The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. "Arbitrary Interference" can also extend to interference provided for under the law.[159]

Article 17 affords protection to personal honor and reputation and States are under an obligation to provide adequate legislation to that end. Provision must also be made for everyone effectively to be able to protect himself against any unlawful attacks that do occur and to have an effective remedy against those responsible. States parties should indicate in their reports to what extent the honor or reputation of individuals is protected by law and how this protection is achieved according to their legal system.[160]

### 2.6.2.General Comment on the right to privacy under Article 17 of the ICCPR

The international human rights community has begun the process of responding to the erosion of privacy rights that these information technologies have facilitated.

---

[155] Martin Scheinin, 'International Covenant on Civil and Political Rights: Key elements in the context of the LIBE Committee inquiry' page 1, 14 October 2013
[156] Martin Scheinin, 'International Covenant on Civil and Political Rights: Key elements in the context of the LIBE Committee inquiry' page 2, 14 October 2013
[157] Martin Scheinin, 'International Covenant on Civil and Political Rights: Key elements in the context of the LIBE Committee inquiry' page 2, 14 October 2013
[158] *Ibid, page 2*
[159] *Ibid, page 3*
[160] *Ibid, page 4*

The U.N. Human Rights Committee should assist in this process by issuing a new General Comment on the right to privacy under Article 17 of the ICCPR.[161]

General Comments are issued by treaty-based bodies that are established by the treaty itself. The HRC is mandated by Article 28 of the ICCPR.

In General Comment 16 the Committee held that processing of personal data in both the public and private sectors must be regulated in accordance with basic data privacy principles.[162]

Strength of international human rights law on privacy erodes when its protections only derive meaning from a world without modern electronic communications and technology. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said: "inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications." The same is true of inadequate international legal frameworks.[163]

General Comment 16 is necessary

**1.** to clarify the contours of the protections now afforded by the right to privacy

**2.** to reflect changing realities

**3.** to ensure continued protection of privacy and other related rights in the world today [164]

General Comment 16 provides some important analysis of the components of Article 17 protections, it is a limited exposition of a complex right. Understandably, it fails to anticipate or account for modern technological developments that have

[161] Privacy Rights in The Digital Age :A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights, March 2014, page 12

[162] Privacy Rights in The Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights, March 2014, page 14

[163] *Ibid, page 16.*

[164] *Ibid, page 18.*

rapidly, drastically, and fundamentally changed the nature of privacy and the relationship between public and private spheres.[165]

### 2.6.3. ECHR Article 8

Whereas ICCPR Article 1 7 is framed essentially in terms of a prohibition on Interference with privacy, ECHR Article 8 is framed in terms of a right to, inter alia, 'respect for private life' followed by an enumeration of criteria permitting interference with that right:

1. Everyone has the right to respect for his private and family life, his home, and correspondence.[166]
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.[167]

The right to privacy is guaranteed in Article 8 of the ECHR (European Convention on Human Rights) and Article of the Charter (Charter of Fundamental rights). The wording of both provisions is similar. Article 8(1) of the ECHR State:

'Everyone has the right to respect for his private and family life, his home, and correspondence'.[168]

Article 7 of the Charter state that:

'Everyone has the right to respect for his private and family life, his home and communications.'[169]

Both articles are protecting the right to private correspondence and communication respectively. Article 7 of the charter covered all form of the

[165] Ibid, page 22.
[166] Article 8 (1) of the European Convention on Human Rights, (ECHR)
[167] Article 8 of the European Convention on Human Rights, (ECHR)
[168] Article 8 (1) of the European Convention on Human Rights, (ECHR),
[169] Article 7 of the Charter of Fundamental Rights (Charter)

communications includings letters, phone calls, and emails. This right has been successfully used to challenge the bugging of phones by public authorities.[170]

The collection and storage of personal information relating to the applicants telephone, as well as to his email and internet usage, withought his knowledge automated to an interference with his right to respect for private life and correspondence within the meaning of Article 8 of the ECHR.[171]

Article 8 of the ECHR is a qualified right. it means that interference with this right can be justified in certain circumstances. Article 8(2) of the ECHR states: "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 securit 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.**[172]**

Where the interference falls within Article 8 (2) of ECHR, there is no breach of Article 8. Interference can only be justified if it is 'in accordance with the law'. This means generally that there has to be a clear legal basis for the interference and that the law should be readily accessible. In the context of secret surveillance, 'in accordance with the law[5] means that member states must insert legal protections against arbitrary interference into their domestic law.**[173]**

### 2.6.4. Article 13 of the ECHR

Article 13 of the ECHR also relevant for data privacy. Article 13 states:

*"Everyone whose rights and freedoms as set forth in the 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."*[174]

---

[170] Lee A. Bygrave, Data Privacy Law: An International Perspective 87 (Oxford University Press, United Kingdom, 1st edn. 2014).
[171] Ibid, page 88
[172] Ibid, page 88
[173] Lee A. Bygrave, Data Privacy Law: An International Perspective 89 (Oxford University Press, United Kingdom, 1st edn. 2014).
[174] Article 13 of the European Convention on Human Rights, (ECHR).

A similar provision is to be found in Article 47 of the EU Charter of Fundamental Rights:

"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article."[175]

The primary aim of these provisions is to increase judicial protection offered to individuals who wish to complain about an alleged violation of their human rights.

These articles are provided effective remedy on the breach of data privacy. According to this article it is the duty of members state to constitute a national authority or tribunals, which provide effective remedy for the breach of data privacy.

[175] Article 47 of the European Convention on Human Rights, (ECHR).

## Part B: National Perspectives -

### 2.7. Introduction

The right to privacy is not new. It has been a common law concept, and an invasion of privacy gives a right to the individual to claim tort-based damages. One of first cases on the said topic was Semayne's Case (1604)[176]. The case related to the entry into a property by the Sheriff of London in order to execute a valid writ. Sir Edward Coke, while recognizing a man's right to privacy famously said that "the house of everyone is to him as his castle and fortress, as well for his Defence against injury and violence, as for his repose". The concept of privacy further developed in England in the 19th century and has been well established in today's world. In case of Campbell v. MGN[177], the court held that if "there is an intrusion in a situation where a person can reasonably expect his privacy to be respected, that intrusion will be capable of giving rise to liability unless the intrusion can be justified".[178]

The advancement of the technology and the dynamism of legal world provides outlook of privacy and data protection issues in this recent era. Privacy is something that is not to interfere to the interest of others. Privacy is becoming a concern of every individual due to technological advancement and it also emphasizes narrowly for protection of data. Data protection emphasis individual liberty and these individual's liberty is under threat by the interference of the stranger.[179]

Over last couple of years there has been a substantial increase in the amount of data that is generated through the usage of various electronic devices and applications. Today's businesses derive a substantial value by analyzing the 'big data' and often determine their business strategies based on such analysis. While there is no denying the business efficiency involved, the burning question is 'do individuals have a

[176] Peter Semayne v Richard Gresham, 77 ER 194,
[177] 2004 UKHL 22.
[178] Uday Shankar, "Privacy and Data Protection Laws in India: A Right Based Analysis" 21 Bharti Law Review 55 (2016)
[179] Uday Shankar, "Privacy and Data Protection Laws in India: A Right Based Analysis" 21 Bharti Law Review 54 (2016)

control over the manner in which information pertaining to them is accessed and processed by others.[180]

Privacy is the right to be left alone or to be free from misuse or abuse of one's personality. The right of privacy is the right to be free from unwarranted publicity, to live a life of seclusion, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.

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.[181]

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, Aadhaar Act 2016, 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. Recently Data (Privacy And Protection) Bill, 2017, 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. etc. This Bill provides for a framework to address the issue on data protection and protect the privacy of all persons These Bill is not sufficient to dispose off the data privacy matters.

[180] Jayanta Ghosh "Data Protection & Privacy Issues in India" Economic Laws Practice 03 (2017),
[181] Noriswadi Ismail and Edwin Lee Yong Cieh, et. at (eds.), *Beyond Data Protection* 6 (Springer, London, 2013)

In the case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[182] 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*."

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.

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 digitalization, 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

[182] 2017(10) SCALE 1

providing individuals full control over their personal data, while ensuring a high level of data protection.[183]

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

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 and others laws". While Privacy issue deals with Article 21 Constitution of India.

## 2.8. The Indian Constitutions 1949

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.

The constitution of India has some provisions like, 'Freedom of Speech and Expression' and 'Right to Life and Personal Liberty' These provisions has 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.

Before the case of ***K. S. Puttaswamy and Others Vs. Union of India***[184] 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

[183] Suneeth Katarki, "The Personal Data Protection Bill, 2018 Key Features and Implications" *Indus law (August 2018).*
[184] 2017(10) SCALE 1

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.

Article 19(1) (a) stipulates that

"*All citizens shall have the right to freedom of speech and expression".*[185]

However, this is qualified by Article 19(2) which states that this shall

*"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, decency or morality, or in relation to contempt of court, defamation or incitement to an offence*".[186]

Thus, the freedom of expression guaranteed by Article 19(1) (a) is not absolute, but a qualified right that is susceptible, under the Constitutional scheme, to being curtailed under specified conditions.

Article 21 provided that

*"No person shall be deprived of his life or personal liberty except according to procedure established by law."*[187]

Article 21 only requires a "*procedure established by law*" as a pre-condition for the deprivation of life and liberty.

Words life or personal liberty also include the privacy. Present time privacy is three kinds of privacy. First kind of privacy is Physical Privacy, second kind of privacy is Territorial Privacy and third is Data Privacy.

[185] Article 19 (1) (a) "The Constitution of India" (1949)
[186] Article 19 (2) "The Constitution of India" (1949).
[187] Article 21 "The Constitution of India" (1949).

Recently in case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[188] 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 Other***[189]***s*** supreme court of India in case of ***M P Sharma v Satish Chandra, District Magistrate, Delhi***[190] and ***Kharak Singh v State of Uttar Pradesh***[191], said that the right to privacy is not protected under the Indian constitution.

The movement towards the recognition of right to privacy in India started with ***Kharak Singh vs The State of U.P***.[192] 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 decided a case — one of the first of its kind on wiretapping. In ***R. M. Malkani vs State of Maharashtra***[193] 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

[188] 2017 (10) SCALE 1
[189] 2017 (10) SCALE 1
[190] 1954 SCR 1077
[191] AIR 1963 SC 1295
[192] AIR 1963 SC 1295
[193] AIR 1973 SC 157

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***[194] 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***[195]**.** 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. The case related to the alleged autobiography of Auto Shankar who was convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various police 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***[196] the court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right

[194] (1975)2 SCC 148
[195] (1994)6 SCC 632
[196] AIR 1997 SC 568

to privacy. The Supreme court held: 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.

Finally, Supreme Court of India in case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[197] decided that the decision of ***M P Sharma v Satish Chandra, District Magistrate, Delhi***[198] and ***Kharak Singh v State of Uttar Pradesh***[199], 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.

Although there is no specific legislation in India which deals with data privacy, but there are variety of laws that will be applicable. Each problem of data privacy is discussed with different set of laws.

## 2.9. Information and Technology Act, 2000

India passed the Information Technology Act 2000 in May 2000 in pursuance of the United Nations General Assembly Resolution A/RES/51/162 of 30th January 1997. This Resolution adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. The Information Technology Act, 2000 came into force on 17th October 2000 and it has been substantially amended through the Information Technology (Amendment) Act, 2008.

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

[197] 2017(10) SCALE 1
[198] 1954 SCR 1077
[199] (1964) 1 SCR 334.

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 in following manner.

The IT Act, after its amendments in 2008, is now equipped with multiple provisions catering to data protection, mandatory privacy policies, and penalties to be imposed on breach of such privacy policies. Following are the relevant provisions of the IT Act:

### 2.9.1. Section 43 of the Information Technology Act, 2000

It provides the provision related to Penalty and compensation for damage to computer, computer system, etc.

*If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, –*

*(a) accesses or secures access to such computer, computer system or computer network or computer resource*[200]

*b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium*[201]

*(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network*[202]

This section provides that any person, who without the permission of the owner or, any other person who may be in charge of a computer, computer system or computer network-

[200] Section 43 (a) of the Information Technology Act,2000 (Act NO. 21 of 2000)
[201] Section 43 (b) of the Information Technology Act,2000 (Act NO. 21 of 2000)
[202] Section 43 (c) of the Information Technology Act,2000 (Act NO. 21 of 2000)

a) accesses or secures access to such computer, computer system or computer network

b) downloads, copies, or extracts any data, computer data base or information from such computer, computer system or computer network which includes information or data held or stored in any removal 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 an intention to cause damage shall be liable to pay damages.

shall be liable to pay damages by way of compensation not exceeding the sum of INR 1,00,00,000 (Rupees One Crore) to the person so affected.

### 2.9.2. Section 43-A of the Information Technology Act, 2000

It provides the provision related to Compensation for failure to protect data.

*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.*[203]

This section is bedrock of data protection and provides that where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, which shall not exceed a sum of INR 5,00,00,000 (Rupees Five Crore).

[203] Section 43-A of the Information Technology Act,2000 (Act NO. 21 of 2000)

Here "Body Corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities[204].

Here "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.[205]

Here "Reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.[206]

### 2.9.3. Section 66-C of the Information Technology Act, 2000

It provides the provision related to Punishment for identity theft.

*"Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person……*[207]

This section deals with identity theft. It provides that if any person, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment for a term which may extend up to three years and shall also be liable to pay a fine of up to Rupees One Lakh.

### 2.9.4. Section 66-E of the Information Technology Act, 2000

Section 66E is of utmost importance. Privacy violation of a person without his consent has been made punishable by virtue of this provision

[204] Explanation (1) of Section 43-A of the Information Technology Act,2000 (Act NO. 21 of 2000)
[205] Explanation (3) of Section 43-A of the Information Technology Act,2000 (Act NO. 21 of 2000)
[206] Explanation (2) of Section 43-A of the Information Technology Act,2000 (Act NO. 21 of 2000)
[207] Section 66-C of the Information Technology Act,2000 (Act NO. 21 of 2000)

Its provide provisions related to Punishment for violation of privacy. This section provides

"*Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both"*[208]

This section provides that whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy27 of that person shall be punished with imprisonment which may extend up to three years or with fine not exceeding Rupees Two Lakh or with both.

Here the word "Captures" with respect to an image, means to videotape, photograph, film or record by any means.[209]

Word "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons.[210]

Word "publishes" means reproduction in the printed or electronic form and making it available for public.[211]

### 2.9.5. Section 72 of the Information Technology Act, 2000

This section provided that Penalty for Breach of confidentiality and privacy.

This section provided that,

*" if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book,*

[208] Section 66-E of the Information Technology Act,2000 (Act NO. 21 of 2000)
[209] Explanation (b) of Section 66-E of the Information Technology Act,2000 (Act NO. 21 of 2000)
[210] Explanation (a) of Section 66-E of the Information Technology Act,2000 (Act NO. 21 of 2000)
[211] Explanation (d) of Section 66-E of the Information Technology Act,2000 (Act NO. 21 of 2000)

*register, correspondence, information, document or other material to any other person…"*[212]

This section provides that Penalty for Breach of confidentiality and privacy. According to this section when any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and thereafter, discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to One Lakh rupees , or with both.

### 2.9.6. Section 72-A of the Information Technology Act, 2000

Section 72-A of this act provided that the provisions related to the Punishment for disclosure of information in breach of lawful contract. In this section fallowing provision provided that,

*"any person including an intermediary who, while providing services under the terms of 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.."*[213]

Section 73-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.

Here the term "intermediary" with respect to any particular electronic records, has been defined to mean any person whose on behalf of another person receives,

[212] Section 72 of the Information Technology Act,2000 (Act NO. 21 of 2000)
[213] Section 72-A of the Information Technology Act,2000 (Act NO. 21 of 2000)

stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online education sites, online market places and cyber cafes.

### 2.9.7. Section 66-F of the Information Technology Act, 2000

Section 66-F provided provisions for Punishment for cyber terrorism.

*Whoever,*

*(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –*

*(i) denying or cause the denial of access to any person authorised to access computer resource; or*

*(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or*

*(iii) Introducing or causing to introduce any Computer Contaminant.*

*and by means ……commits the offence of cyber terrorism.*[214]

Cyber terrorism which has been made more proliferate by social media has also been made punishable by Section 66-F of the Act.

### 2.9.8. Section 67 of the Information Technology Act, 2000

Its provided that's "Punishment for publishing or transmitting obscene material in electronic form."

According to this section,

*"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied*

[214] Section 66-F of the Information Technology Act,2000 (Act NO. 21 of 2000)

*in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees."*[215]

Obscenity in electronic form which is very much prevalent on social media website will come under Section 67 of the Act, which makes it punishable to transmit or publish any obscene material.

### 2.9.9. Section 67A of the Information Technology Act, 2000

Section 67A provides punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

## 2.10. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011

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.

### 2.10.1. Rule 4

Rule provided that provisions related to "Body corporate to provide policy for privacy and disclosure of information"

"*The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that*"[216]

[215] Section 67 of the Information Technology Act,2000 (Act NO. 21 of 2000)
[216] Sub-rule (i) Rule 4, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

This rule provided duty of corporate bodies or any persons who on behalf of body corporate receives, stores, deals, collects, possess, or handle information's. it is the duty of that corporate bodies or that persons to provide privacy policy, published this policy on website and ensure that this policy are fallowed. When privacy policy published shall provide

(a) clear and easily accessible statements of its practices and policies[217]

(b) personal or sensitive personal data or information collected under rule 3.[218]

(c) purpose of collection and usage of such information[219]

(d) disclosure of information including sensitive personal data or information as provided in rule 6.[220]

(e) reasonable security practices and procedures as provided under rule 8.[221]

**2.10.2. Rule 5**

This rule lays down the procedure to be followed for the collection of information by the body corporate or any person on its behalf.

According to this rule, Consent has to be obtained in writing through letter or fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.[222]

It is the duty of the body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

[217] Sub-rule (i) (i) Rule 5of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[218] Sub-rule (i) (i) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[219]Sub-rule (i) (iii) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[220] Sub-rule (i) (iv) Rule 5of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[221] Sub-rule (i) (v) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[222] Sub-rule (i) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf[223]

b) the collection of the sensitive personal data or information is considered necessary for that purpose.[224]

it is the duty of the body corporate or any person on its behalf, while collecting information directly from the person concerned, shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

**a)** Fact that the information is being collected[225]

**b)** Purpose for which the information is being collected[226]

**c)** Intended recipients of the information[227]

**d)** Name and address of

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.[228]

It is the duty of the the body corporate or any person on its behalf, when they holding their sensitive personal data or information cannot not retain that information for longer than is required for the purpose for which the information may lawfully be used or is otherwise required under any other law for the time being in force.[229] The

[223] Sub-rule (ii) (a) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[224]Sub-rule (ii) (b) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011""

[225] Sub-rule (iv) (a) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[226]Sub-rule (iv) (b) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011""

[227] Sub-rule (iv) (c) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[228] Sub-rule (iii) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[229] Sub-rule (iv) rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

information collected can only be used for the purpose for which it has been collected.[230]

It is the obligations on Body corporate or any person on its behalf shall permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient is corrected or amended as feasible. However, a body corporate is not responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such boy corporate or any other person acting on behalf of such body corporate.[231]

It is duty of the Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing its consent, the body corporate has the option not to provide goods or services for which the said information was sought.[232]

It is the mandatory duty of the Body corporate or any person on its behalf is required keep the information secure as provided in rule 8.[233]

### 2.10.3. Rule 6

This rule pertains to the disclosure of information by the body corporate to any third party. The body corporate or any person on its behalf cannot publish the sensitive personal data or information.[234]

---

[230] Sub-rule (v) rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[231] Sub-rule (vi) Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[232] Sub-rule (vii) of Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[233] Sub-rule (viii) of Rule 5, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

Rule 6 provide that, it is the duty of the body corporate when he disclosure of sensitive personal data or information of the any third it is mandatory requirement that to get prior permission from the provider of such information, who has provided such information under lawful contract or otherwise.[235]

But some conditions it's not require to the body corporate to get prior permission from the information provider,

(i) such disclosure has been agreed to in the contract between the body corporate and provider of information, or

(ii) where the disclosure is necessary for compliance of a legal obligation.[236]

However, its mandatory to share the information, without obtaining prior consent from provider of information, with Government agencies as mandated under law to obtain information including sensitive personal data or information for the purpose of

(1) verification of identity

(2) for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.[237]

In this regards the Government agency has to send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.[238]

---

[234] Sub-rule (iii) of Rule 6, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[235] Sub-rule (i) of Rule 6, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[236] Ibid.

[237] Sub-rule (i) of Rule 6, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"

[238] Ibid.

Notwithstanding anything contain in such Rule, any sensitive personal data on information can disclosed to any third party by an order under the law for the time being in force.[239]

The third party receiving the sensitive personal data or information from body corporate or any person on its behalf cannot disclose it further.[240]

### 2.10.4. Rule 8

Rule 8 provide provisions related to Reasonable Security, Practices and Procedures of data protection.

According to this rule, While handling such personal information or sensitive personal data or information, it is the mandatory obligations of the corporate body is required to comply with reasonable security practices and procedures.[241]

A body corporate or a person on its behalf is considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security program and information security policies. If they have complied with reasonable security practices and procedures it is the duty of that body corporate or a person on its behalf is contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[242]

In the event of an information security breach, the body corporate or a person on its behalf is required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security program and information security policies.[243]

---

[239] Sub-rule (2) of Rule 6, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[240] Sub-rule (iv) of Rule 6, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[241] Sub-rule (i) of Rule 8, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[242] Sub-rule (i) of Rule 8, of the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011"
[243] Ibid.

## 2.11. Indian Telegraph Act, 1885

### 2.11.1. Section 5 - Power for Government to take possession of licensed telegraphs and to order interception of messages

*"On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act."*[244]

According to section 5, on the occurrence of any "public emergency" or in the interest of the public safety, the central government or a state government, or any authorized officer may take temporary possession of any telegraph established, maintained or worked by any person licensed under the Act.

*"On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing……*[245]

During any such emergency, other necessary orders can be issued in the interest of the sovereignty and integrity of India, the security of the state or for maintaining friendly relations with any foreign state or public order. The regulatory orders can be passed for preventing incitement to the commission of any offence also. In this connection, directions may be given that a particular message, to or from any person or relating to any particular subject, be not transmitted, or be intercepted or be disclosed to the government. Before taking such action, the reasons should be recorded in writing.

[244] Section 5 (1) of the Indian Telegraph Act,1885 (Act No. 13 of 1885)
[245] Section 5 (2) of the Indian Telegraph Act,1885 (Act No. 13 of 1885)

*"Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."*[246]

The press messages intended to be published in India or correspondents accredited to the central government or a state government cannot be ordinarily intercepted or detained.

For the purposes of taking into temporary possession any telegraph, the 'public emergency' includes any situation in which problems arise concerning the public safety, threat to sovereignty and integrity of the country, the security of the state, public order etc. It is in the context of these matters that the appropriate authority has to form an opinion with regard to the occurrence of a 'public emergency' with a view to take temporary possession of any telegraph. Economic emergency is not one of those matters expressly mentioned in the statute.[247]

Moreover, 'economic emergency' may not necessarily amount to a public emergency and justify action under this section unless it raises problems relating to the abovementioned matters.

### 2.11.2. Section 24 – Unlawfully attempting to learn the contents of messages

*"If any person does any of the acts mentioned in section 23 with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under this Act, he may (in addition to the fine with which he is punishable under section 23) be punished with imprisonment for a term which may extend to one year."*[248]

This section provides for the consequences of attempting to learn the contents of messages unlawfully. If any person does any of the acts mentioned in section 23 with the intention of unlawfully learning the contents of any message, or any person

[246] Proviso of Section 5 (1) of the Indian Telegraph Act,1885 (Act No. 13 of 1885)
[247] Uday Shankar, "Privacy and Data Protection Laws in India: A Right Based Analysis" 26 Bharti Law Review 55 (2016)
[248] Section 24 of the Indian Telegraph Act,1885 (Act No. 13 of 1885)

unlawfully attempts to learn contents of a message, he may be punished with a fine of five hundred rupees with imprisonment for a term which may extend to one year.

### 2.11.3. Section 25 – Intentionally damaging or tampering with telegraphs

*If any person, intending*

*a) to prevent or obstruct the transmission or delivery of any message, or*

*(b) to intercept or to acquaint himself with the contents of any message, or*

*(c) to commit mischief,*

*damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof, he shall be punished with imprisonment for a term which may extend to three years, or with fine or with both.*[249]

The section provides for the consequences of intentionally damaging or tampering with telegraphs. If any person, intending to prevent or obstruct the transmission or delivery of any message, or to intercept or to acquaint himself with the contents of any message, or to commit mischief, damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof, shall be punished with imprisonment for a term which may extend to three years, or with fine or with both.

### 2.11.4. Section 26 – Telegraph officer or other official making away with or altering, or unlawfully intercepting or disclosing messages, or divulging purport of signals

*If any telegraph officer, or any person, not being a telegraph officer, but having official duties connected with any office which is used as a telegraph office*

*(a) willfully, secrets, makes away with or alters any message which he has received for transmission or delivery, or*

*(b) willfully, and otherwise than in obedience to an order of the Central*

[249] Section 24 of the Indian Telegraph Act,1885 (Act No. 13 of 1885)

*Government or of a State Government, or of an officer specially authorized [by the Central or a State Government] to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent Court, discloses the contents or any part of the contents of any message, to any person not entitled to receive the same, or*

*(c) divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same,*

*he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.*[250]

This section provided that, if any telegraph officer, or any person, not being a telegraph officer but having official duties connected with any office which is used as a telegraph office, willfully, secrets, makes away with or alters any message which he has received for transmission or delivery, or willfully, and otherwise than in obedience to an order of the Central Government or of a State Government, or of an officer specially authorized by the Central or a State Government to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent court, discloses the contents or any part the contents of any message, to any person not entitled to receive the same, or divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same, shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.[251]

### 2.11.5. Section 30 – Retaining a message delivered by mistake

The section provides that, if any person fraudulently retains, or willfully secretes, makes away with or detains a message which ought to have been delivered to some other person, or, being required by a telegraph officer to deliver up any such

[250] Section 25 of the Indian Telegraph Act,1885 (Act No. 13 of 1885)
[251] Uday Shankar, "Privacy and Data Protection Laws in India: A Right Based Analysis" 27 Bharti Law Review 55 (2016)

message, neglects of refuses to do so, shall be punished with imprisonment for a term which may extend to two years, or with fine, or with both.[252]

## 2.12. Banking Regulations

### 2.12.1. State Bank of India Act, 1955

#### 2.12.1.1. Section 44 – Obligation as to fidelity and secrecy

*"The state bank shall observe, except as otherwise required by law, the practice and usages customary among bankers ……. Necessary or appropriate for the state bank to divulge such information."*[253]

This section provides for a secrecy clause by virtue of which, the bank as a whole and its directors, local boards, auditors, advisers, officers or other employees of the State Bank are obligated as to fidelity and secrecy, by a declaration in prescribed form.

It provides that, the State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary among bankers, necessary or appropriate for the State Bank to divulge such information.

### 2.12.2. Banking Companies (Transfer and Acquisition of Undertakings) Act, 1980

#### 2.12.2.1. Section 13 – obligations as to fidelity and secrecy

**"***Every corresponding new bank shall observe, except as otherwise required by law, the practice and usages customary among bankers …….. Necessary or appropriate for the state bank to divulge such information"*[254]

[252] Section 30 of the Indian Telegraph Act,1885 (Act No. 13 of 1885)
[253] Section 44 of the State Bank of India Act,1955 (Act No. 23 of 1955)
[254] Section 13 of the Banking Companies (Transfer and Acquisition of Undertakings) Act, 1970 (Act No. 5 of 1970)

This section provides that, every corresponding new bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with law or practices and usages customary among bankers, necessary or appropriate for the corresponding new bank to divulge such information.[255]

Section 13 (2) provide that

*"Every director, members of a local board or a committee, or auditor adviser or other employee of a corresponding new bank shall, before entering upon his duty, make a declaration of fidelity and secrecy in the form set out in Third Schedule."*[256]

Further, every Director, member of a local Board or a committee, or Auditor, Adviser, officer or other employee, custodian of a corresponding new bank shall, before entering upon his duties, make a declaration of fidelity and secrecy in the prescribed form.[257]

### 2.12.3. Credit Information Companies (Regulation) Act, 2005 ("CIC Act")

#### 2.12.3.1. Section 19 – Accuracy and security of credit information

Section 19 provided that,

*"A credit information company or credit institution or specified user, as the case may be, in possession or control of credit information, shall take such steps (including security safeguards) as may be prescribed, to ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorized access or use or unauthorized disclosure thereof."*[258]

[255] Section 13 (1) of the Banking Companies (Transfer and Acquisition of Undertakings) Act, 1970 (Act No. 5 of 1970)
[256] Section 13(2) of the Banking Companies (Transfer and Acquisition of Undertakings) Act, 1970 (Act No. 5 of 1970)
[257] Section 13 (3) of the Banking Companies (Transfer and Acquisition of Undertakings) Act, 1970 (Act No. 5 of 1970)
[258] Section 19 of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)

This section requires a credit information company[259], credit institutions and specified users[260] to take steps in order preserve accuracy and security of credit information[261], to ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

### 2.12.3.2. Section 20 – Privacy principles

This section provides privacy Principles, that every credit information company, credit institutions and specified users shall adopt privacy principles in relation to credit information and shall adopt the following privacy principles in relation to collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information, namely,[262]

a) the principles—

(i) which may be followed by every credit institution for collection of information from its borrowers and clients and by every credit information company, for collection of information from its member credit institutions or credit information companies, for processing, recording, protecting the data relating to credit information furnished by, or obtained from, their member credit institutions or credit information companies, as the case may be, and sharing of such data with specified users[263]

---

[259] The term "**credit information company**" has been defined to mean a company formed and registered under the Companies Act, 1956 (1 of 1956) and which has been granted a certificate of registration under sub-section (2) of section 5.

[260] The term **"specified user**" has been defined to mean any credit institution, a credit information company being a member under subsection (3) of section 15, and includes such other person or institution as may be specified by regulations made, from time to time, by the Reserve Bank for the purpose of obtaining credit information from a credit information company. 39

[261] The term "**credit information**" has been defined to mean any information relating to—(i) the amounts and the nature of loans or advances, amounts outstanding under credit cards and other credit facilities granted or to be granted, by a credit institution to any borrower; (ii) the nature of security taken or proposed to be taken by a credit institution from any borrower for credit facilities granted or proposed to be granted to him; (iii) the guarantee furnished or any other non-fund based facility granted or proposed to be granted by a credit institution for any of its borrowers; (iv) the credit worthiness of any borrower of a credit institution; (v) any other matter which the Reserve Bank may, consider necessary for inclusion in the credit information to be collected and maintained by credit information companies, and, specify, by notification, in this behalf.

[262] Section 20 of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)

[263] Section 20 (a)(i) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)

(ii) which may be adopted by every specified user for processing, recording, preserving and protecting the data relating to credit information furnished, or received, as the case may be, by it[264]

(iii) which may be adopted by every credit information company for allowing access to records containing credit information of borrowers and clients and alteration of such records in case of need to do so[265]

b) the purpose for which the credit information may be used, restriction on such use and disclosure thereof[266]

c) the extent of obligation to check accuracy of credit information before furnishing of such information to credit information companies or credit institutions or specified users, as the case may be[267]

d) preservation of credit information maintained by every credit information company, credit institution, and specified user as the case may be (including the period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information)[268]

e) networking of credit information companies, credit institutions and specified users through electronic mode[269]

f) any other principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations.[270]

### 2.12.3.3. Section 22 – Unauthorized access to credit information

This section provides that

*"No person shall have access to credit information in the possession or control of a credit information company or a credit institution or a specified user*

[264] Section 20 (a)(ii) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005
[265] Section 20 (a)(iii) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005
[266] Section 20 (b) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005
[267] Section 20 (c) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005
[268] Section 20 (d) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005
[269] Section 20 (e) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)
[270] Section 20 (f) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)

*unless the access is authorized by this Act or any other law for the time being in force or directed to do so by any court or tribunal and any such access to credit information without such authorization or direction shall be considered as an unauthorized access to credit information."*[271]

If any person unauthorized access to credit information in the possession or control of a credit information company or a credit institution or a specified user shall be punishable with fine which may extend to INR 1,00,000 (Rupees One Lakh) in respect of each offence and if he continues to have such unauthorized access, with further fine which may extend to INR 10,000 (Rupees Ten Thousand) for every day on which the default continues and such unauthorized credit information shall not be taken into account for any purpose.[272]

### 2.12.3.4. Section 29 – Obligations as to fidelity and secrecy

This section provides for secrecy and fidelity to be maintained by every credit information company. Its provided that,

*"Every credit information company shall observe, except as otherwise required by law, the practices and usages customary among credit information companies and it shall not divulge any information relating to, or to the affairs of, its members or specified users."*[273]

This section provides for secrecy and fidelity to be maintained by every credit information company with respect to the credit information except as otherwise required by law, the practices and usages customary among credit information companies and it shall not divulge any information relating to, or to the affairs of, its members or specified users.

Further, its provided that,

*"Every chairperson, director, member, auditor, adviser, officer or other employee of a credit information company shall, before entering upon his duties,*

[271] Section 22 (1) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)
[272] Section 22 (2) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)
[273] Section 29 (1) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)

*make a declaration of fidelity and secrecy in the form, as may be prescribed in this regard".*[274]

Section 29 clause (2) provide provision that, it is the duty of every chairperson, director, member, auditor, adviser, officer or other employee of a credit information company shall, before entering upon his duties, make a declaration of fidelity and secrecy.

### 2.12.4. Credit Information Companies Regulations, 2006 ("CIC Regulations")

#### 2.12.4.1. Regulation 10 of CIC Regulations

In this regulation it specifies that, in addition to section 20 of the CIC Act, every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to their functioning, namely,[275]

a) Care in collection of credit information properly and accurately recorded, collated and processed, protected against loss, unauthorized access, use, modification or disclosure thereof.[276]
b) Keep the credit information furnished by it updated, accurate and complete[277]
c) Establish and adopt procedures relating to disclosure to a person, upon his request, his own credit information and subject to his satisfactory identification[278]
d) Retain credit information collected, maintained and disseminated by them for a minimum period of seven years[279]
e) Develop guidelines and procedures to be adopted by them, with the approval of the Reserve Bank of India in respect of preservation and destruction of credit information.[280]

#### 2.12.4.2. Regulation 11 of CIC Regulations

In This regulation it provided that, principles and procedures relating to personal data. Every credit information company, credit institution and specified user, shall adopt the following principles,[281]

[274] Section 29 (2) of the Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)
[275] Regulation 10 of the Credit Information Companies Regulations, 2006
[276] Regulation 10 (a) of the Credit Information Companies Regulations, 2006
[277] Regulation 10 (b) of the Credit Information Companies Regulations, 2006
[278] Regulation 10 (c) of the Credit Information Companies Regulations, 2006
[279] Regulation 10 (d) of the Credit Information Companies Regulations, 2006
[280] Regulation 10 (e) of the Credit Information Companies Regulations, 2006

a) Personal data shall not be collected, or published or disclosed except for the purposes relating to their functions under the CIC Act, or in relation to their capacity and function as an employer of an individual who is or has been in their employment[282]

b) Ensure that, before such data is collected or, if that is not practicable, as soon as practicable after such data is collected, the individual concerned is informed about such collection, and such data maintained by the should be protected against any loss, or unauthorized access, or use, or modification or disclosure, thereof[283]

c) Retain personal data collected, maintained and disseminated by them for a minimum period of seven years,[284]

d) Develop guidelines and procedures to be adopted by them, with the approval of the Reserve Bank of India in respect of preservation and destruction of such personal data.[285]

### 2.12.5. The Public Financial Institutions (Obligation as To Fidelity and Secrecy) Act, 1983 ("PFI Act")

Section 3 of this act provides that,

Any public financial institution shall not, except as otherwise provided in any other law for the time being in force, divulge any information relating to, or to the affairs of, its constituents except in circumstances in which it is, in accordance with the law or practice and usage, customary among bankers, necessary or appropriate for the public financial institution to divulge such information.[286]

**Section 4** of this act provides that,

Every director, member of any committee, auditor or officer or any other employee of a public financial institution to which the PFI Act applies, shall, before

[281] Regulation 11 of the Credit Information Companies Regulations, 2006
[282] Regulation 11(a) of the Credit Information Companies Regulations, 2006
[283] Regulation 11(b) of the Credit Information Companies Regulations, 2006
[284] Regulation 11(c) of the Credit Information Companies Regulations, 2006
[285] Regulation 11(d) of the Credit Information Companies Regulations, 2006
[286] Section 3 of the "The Public Financial Institutions (Obligation as To Fidelity and Secrecy) Act, 1983" (Act No. 12 of 1983).

entering upon his duties make a declaration of fidelity and secrecy in the form set out in the PFI Act.[287]

## 2.13. Medicine and Healthcare

### 2.13.1. The Mental Health Act, 1987

#### 2.13.1.1. Section 13 - Inspection of psychiatric hospitals and psychiatric nursing homes and visiting of patients

This section provided that duty of psychiatric hospitals and psychiatric nursing homes and rights of the Inspecting officer.

*"An Inspecting Officer may, at any time, enter and inspect any psychiatric hospital or psychiatric nursing home and require the production of any records, which are required to be kept in accordance with the rules made in this behalf, for inspection"*[288]

This section provides for inspection of psychiatric hospitals and psychiatric nursing homes and visiting patients by an inspecting officer at any time and the inspecting officer may require the production of any records maintained as per the MH Act.

*"Provided that any personal records of a patient so inspected shall be kept confidential except for the purposes of sub-section (3)*[289]*".*

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.[290]

---

[287] Section 4 of the "The Public Financial Institutions (Obligation as To Fidelity and Secrecy) Act, 1983" (Act No. 12 of 1983).
[288] Section 13(1) of the "The Mental Health Act, 1987" (Act No. 14 of 1987)
[289] Proviso of Section 13(1) of the "The Mental Health Act, 1987" (Act No. 14 of 1987)
[290] Section 13(3) of the "The Mental Health Act, 1987" (Act No. 14 of 1987)

#### 2.13.1.2. Section 38 – Monthly inspection by Visitors

Section 38 provide provisions related to the monthly inspection by the visitors. According to this section visitors do monthly inspections in the psychiatric hospital on psychiatric nursing home, and see the data of the patients. But visitors of psychiatric patients will not be entitled to inspect any personal records of an in-patient which in the opinion of the medical officer-in-charge are confidential in nature.[291]

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

In This regulation, Regulation 7.14 provides that,

It is the duty of the medical practitioner to maintain the secrecy. The registered medical practitioner shall not disclose the secrets of a patient that have been learnt in the exercise of his profession.[292]

But in fallowing circumstances they are free to disclosed the secrecy of the patient, in the pursuance of orders of the presiding judge in a court of law.

**I.** It is a serious and identified risk to a specific person or community and

**II.** It is notifiable diseases.

In case of communicable or notifiable diseases, concerned public health authorities should be informed immediately.[293]

### 2.14. Insurance

#### 2.14.1. Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017

Regulation 9 of this regulation provides the obligations on referral company[294]. According to this regulation a referral company who is approved by the Insurance Regulatory and Development Authority of India (IRDAI) and registered

[291] Section 38 of the "The Mental Health Act, 1987" (Act No. 14 of 1987)
[292] Regulations 7.14 of the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
[293] Ibid.
[294] The term "**Referral Company**" has been defined to mean a company formed and registered under the Companies Act, 1956 and approved by the IRDAI under sub-regulation (3) of regulation 6 except as otherwise permitted in these regulations.

with the insurer will not provide details of customers without their prior written consent or provide details of any person or firm or company with whom they have not had any recorded business transaction.[295]

### 2.14.2. Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015

Regulation 3 of This regulation provided that the duty of insurer to maintain the records. According to this rule every insurer maintaining records of the insurance policies and its relevant data and such a system of maintenance should have the necessary security features. The manner and maintenance of the records shall be as per policy framed by the insurers and approved by their board.[296]

For maintaining records in electronic form, the policy should include:

**a.** Security of hardware and software
**b.** Processing and electronic maintenance of records,
**c.** Backups, disaster recovery and business continuity
**d.** Handling virus, vulnerability issues,
**e.** Privacy and security of policyholder and claim data,
**f.** Data archival.[297]

The policy will also include a detailed plan to review the implementation of the maintenance and storage of records which will be overseen by the risk management committee of the board of the insurers. The records will be held in data centers located and maintained in India only.

### 2.14.3. Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017

These regulations mandate that the board of directors of the insurance to formulate an outsourcing policy wherein assessment of risks involved in outsourcing including the confidentiality of data, quality of services rendered under outsourcing

[295] Regulation 9 of the Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017
[296] Regulation 3 of the Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015
[297] Ibid.

contracts is addressed.[298] Further, the outsourcing agreements are required to contain information and asset ownership rights, information technology, data security and protection of confidential information, contract termination clause specifying orderly handing over of data, assets etc.[299]

Regulations 12 also provided that confidentiality and security measures to be undertaken by the insurers while outsourcing its services. The insurer shall satisfy itself that the outsourcing service provider's security policies, procedures and controls will enable the insurer to protect confidentiality and security of policyholders' information even after the contract terminates. It shall be the responsibility of the insurer to ensure that the data or information parted to any outsourcing service provider under the outsourcing agreements remains confidential. An insurer shall take into account any legal or contractual obligations on the part of the outsourcing service provider to disclose the outsourcing arrangement and circumstances under which insurer's customer data may be disclosed. In the event of termination of the outsourcing agreement, the insurer should ensure that the customer data is retrieved from the service provider and ensure there is no further use of customer data by the service provider.

## 2.15. 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.[300]

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.

[298] Regulations 7 of the Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017.
[299] Regulations 11 of the Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017.
[300] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits And Services) Act, 2016 ((Act No 18 of 2016)

### 2.15.1. Section 28- Security and confidentiality of information

This section provides that subject to the provisions of the Aadhaar Act, the relevant authorities shall ensure the security of identity information and authentication records of individuals.

*"Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals*"[301]

Section 28 (3) provided that,

"*The Authority shall 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 and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.*"[302]

It means 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.

### 2.15.2. Section 29- Restriction on sharing information

This section provided the provisions related to the prohibits the core biometric information.[303]

According to section 29 (1) of the Aadhaar Act,

*"No core biometric information, collected or created under this Act, shall be*

[301] Section 28 (2) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016)
[302] Section 28 (3) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016)
[303] Section 2 (j) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016)
The word "Core biometric information" means finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations.

***(a)*** *shared with anyone for any reason whatsoever; or*

***(b)*** *used for any purpose other than generation of Aadhaar numbers and authentication under this Act."*[304]

This section 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.

The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations.[305]

Sections 29(3) provided that,

*"No identity information available with a requesting entity shall be—*

*(a) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or*

*(b) disclosed further, except with the prior consent of the individual to whom such information relates."*[306]

No identity information available with a requesting entity shall be

**(a)** Used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication[307]

**(b)** disclosed further, except with the prior consent of the individual to whom such information relates.[308]

---

[304] Section 29 (1) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016)
[305] Section 29 (2) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).
[306] Section 29 (3) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).
[307] Section 29 (3)(a) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).
[308] Section 29 (3)(b) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).

No Aadhaar number or core biometric information shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.[309]

**Sections 30 - Biometric information deemed to be sensitive personal information**

This section provided that,

*"The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be "electronic record……"*[310]

This section states that biometric information will be deemed to be sensitive personal information and the provisions contained in the IT Act and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of the Aadhaar Act.

**Section 33- Disclosure of information in certain cases**

Section 33(1) provided that,

*"Nothing contained in sub-section (2) or sub-section (5) of section 28 or sub-section (2) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made pursuant to an order of a court not inferior to that of a District Judge"*

This section provides that information as mentioned in sections 28 and 29 may be disclosed in the event of a pursuant to an order of a court not inferior to that of a District Judge.

But no order issued by the court under this sub-section shall be made without giving an opportunity of hearing to the Authority.

[309] Section 29 (4) of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).
[310] Section 30 of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).

Section 33(2) provided that,

*"……. authentications records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorized in this behalf by an order of the Central Government"*

According to this section, In the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorized in this behalf by an order of the Central Government.

### 2.15.3. Sections 37 - Penalty for disclosing identity information

This section provides for penalty for disclosing identity information.

According to this section,

Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorized under this Act or regulations made thereunder or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.[311]

## 2.16. Aadhaar (Data Security) Regulations, 2016

In this regulation provide provisions related to the data protections. Regulations 3 provide provisions related to data privacy.

This regulation specifies that the authority may specify an information security policy. These policies set out inter alia the technical and organizational measures to be adopted by the authority. This policy and security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and authentication service agencies.

[311] Section 37 of the "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" (Act No 18 of 2016).

Such information security policy may inter-alia provide for

- Controlled access to confidential information
- Restrictions on personnel relating to processes, systems and networks
- Inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the authority.[312]

## 2.17. Aadhaar (Sharing of Information) Regulations, 2016

Regulations 3,4,5 of the Aadhaar (Sharing of Information) Regulations, 2016 are provided provision related to data privacy of the individuals.

According to regulations 3 of this regulations, core biometric information collected by the authority/requesting entity will not be shared with anyone for any reason whatsoever.[313]

According to regulations 4 of this regulations, demographic information and photograph of an individual collected by the authority may be shared with a requesting entity in response to an authentication request for e-KYC data pertaining to such individual, upon the requesting entity obtaining consent from the Aadhaar number holder.[314]

Regulations 5 provided fallowing provisions related to the privacy of Aadhaar. According to these provisions any individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number[315], shall:

**(a)** Collect, store and use the Aadhaar number for a lawful purpose[316]

**(b)** Inform the Aadhaar number holder the following details

i. the purpose for which the information is collected[317]

[312] Regulations 3 of the "Aadhaar (Data Security) Regulations, 2016".

[313] Regulations 3 of the "Aadhaar (Sharing of Information) Regulations, 2016".
[314] Regulations 4 of the "Aadhaar (Sharing of Information) Regulations, 2016".
[315] Regulations 5 of the "Aadhaar (Sharing of Information) Regulations, 2016".
[316] Regulations 5 (a) of the "Aadhaar (Sharing of Information) Regulations, 2016".

ii. whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it[318]

iii. alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any[319]

**(c)** Obtain consent of the Aadhaar number holder to the collection, storage and use of his Aadhaar number for the specified purposes.[320]

Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent and shall not share the Aadhaar number with any person without the consent of the Aadhaar number holder.[321]

## 2.18. Conclusion

The analysis of 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 fundamental right and after analysis; it is justified to treat as right. From others interference and Infringement of individual liberty can only be satisfied the entire legal requirement as a right of data protection. 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, processing, storage, security and access should provide a platform

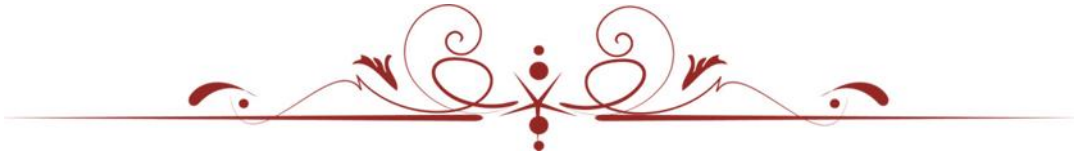
[317] Regulations 5(b)(i) of the "Aadhaar (Sharing of Information) Regulations, 2016".
[318] Regulations 5(b)(ii) of the "Aadhaar (Sharing of Information) Regulations, 2016".
[319] Regulations 5(b)(iii) of the "Aadhaar (Sharing of Information) Regulations, 2016".
[320] Regulations 5(c) of the "Aadhaar (Sharing of Information) Regulations, 2016".
[321] Regulations 5(2) of the "Aadhaar (Sharing of Information) Regulations, 2016".

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. Companies cannot get full protection of data through that which ultimately forced them to enter into separate private contracts to keep their data secured. These contracts have the same enforceability as the general contract.

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. Going by the definition of personal data laid down by the European Union's data protection guidelines, "information concerning an identified and identifiable natural person" covers the scope of personal data. Therefore, if we follow this definition, the personal information provided by individuals during biometrics would be included. 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. The bill has been drafted wholly on the structure of the UK Data Protection Act whereas today's requirement is of a comprehensive Act. Thus it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favorable to the today' requirement.



# Chapter III

# Impact of Social Media on Data Privacy

# Chapter III
# Impact of Social Media on Data Privacy

## 3.1. Introduction

Privacy is a basic human need. It is anthropologically and psychologically rooted in the sense of shame and the need for bodily integrity, personal space, and intimacy in interpersonal relationships. Especially in modern Western cultures, it is understood as a necessary condition for individual autonomy, identity, and integrity.

Technological developments have coincided with significant social change affecting the notion of the privacy. The advent of social media has given everyone a forum in which to disclose personal information on a large and permanent scale. The pervasiveness of social media has challenged individual and societal views of what is or, or should be private. Present time private information of an individual will be disclosed.[322] However, it is the notion of privacy that, in principle, each person maintain control over how much of their personal information become available to others and to whom it should become known.[323]

Present time we are living in Digital Era where everything is digital such as an e-library, e-mail, e-shopping, e-ticket, e-payment, e-governance and many more. People use social media sites for entertainment such as Facebook, Twitter, and You Tube for video, photos, twits, and data downloads as well as uploads in the internet. People use internet for travels and food orders, such as Ola, Uber, Swigi, Zomato, etc and share their personal data to the company. Internet has stored a massive amount of data or information and it is nothing but the Big Data. Dynamic nature of social media data is a significant challenge for continuously and speedily evolving social media sites.

Social media and networks provide powerful systems for businesses to learn and use productively. Based on the pervasive use and prevailing impact social media

[322] Norman Witzleb and David Lindsay, "Emerging Challenges in Privacy Law" 2 (Cambridge University Press, United Kingdom, 2014).
[323] Norman Witzleb and David Lindsay, "Emerging Challenges in Privacy Law" 3 (Cambridge University Press, United Kingdom, 2014).

have on society. Most people have already shared parts of their personal information with several organizations, and have accepted the loss of partial privacy. For example, one may have accepted terms to share personal health information with healthcare networks and insurance agencies, and purchasing power and trends with sales and marketing agencies. However, such data may be shared between the data holders, either due to mergers or data sharing agreements between the organizations. Combination of such data may result in a more complete view of the individual, which may be unacceptable to the concerned individuals, especially if they perceive that it may be used against their interests.

The business world is undergoing a revolution driven by the use of data and analytics to guide decision-making. While many forces are at work, a major reason for the business analytics revolution is the rapid proliferation of the amount of data available to be analyzed. Leading organizations increasingly recognize the importance of leveraging their data as a strategic asset. Some organizations undertake analytics initiatives to improve the quality of customer experience by measuring and acting on sentiments expressed by customers or by linking various divisions and operating units that customers tend to connect with. Others analyze data to predict a customer ‘s propensity to buy new products or services in order to proactively make recommendations for future purchases or offer discounts to encourage a longer-term relationship.

### 3.2. 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.

Social Media are a web-based service that's allow individuals to

**(1)** Construct a public or semi-public profile within a bounded system
**(2)** Articulated a list of other users with whom they share a connection,
**(3)** View and transverse their list of connection and those made by others within the system[324]

### 3.3. Types of Social Media

In this Digital Era, there are many types of social media these are fallowing,

#### 3.3.1. SNS (Social networking sites)

Social networking sites (SNS) are networks enable and help people to connect and interact with each other through a website and to expand their personal networks (e.g., Facebook, Myspace).

#### 3.3.2. Blogs

These are websites function as online personal journals. They enable writers to post their opinions online and allow readers to comment (e.g., Blogger, WordPress).

Examples of popular Social Networking sites are as follows:

#### 3.3.3. Facebook Inc

Facebook Inc. is an American online social media and social networking service company. Facebook service can be accessed from devices with internet connectivity, such as personal computers tablets, and smartphone. After registering, user can create a customized profile revealing information about themselves. They can post text, photo and multimedia which is shared with other users that have agreed to be their friend. User can also use various embedded apps join common interest groups, and receive notifications of their friend's activities.

[324] Daxton R. Stewart, "Social Media and the Law" 9 (Routledge Press, New York, 2017).

It receives prominent media coverage, including many controversies. These often involve user privacy, political manipulation, some content that user find objectionable, including fake news, conspiracy theory, etc.

This application has several public features like

'Marketplace' to post and respond to classified advertisements online;

'Groups' to publicize events and invite guests and friends for attending that event

'Pages' to create and promote a personal or business ideas or involve others in a topic.

### 3.3.4. Tweeter

Twitter is a micro blog service which allows registered members to broadcast and follow replies to short posts, better known as 'Tweets' with no approvals required. Other users can subscribe to follow or reply to the tweets which may include hyperlinks to other blogs or posts and receive update messages by adding 'Hashtags' to keyword on the post, this acts like a metatag, expressed as #keyword. The tweets are searchable and available for the public. Twitter works on Ruby-for Rails which is an open source web framework and its API is available for application developers.

### 3.3.5. LinkedIn

LinkedIn is designed primarily for corporate business community to promote personal brand online and allows registered members to establish a network of other professionals whom they know and trust as 'connections'. This requires preexisting relationships unlike Facebook or Twitter. Educational and Professional qualifications are the main display items on user pages here.

### 3.3.6. Google+ -

Google+ provides ability to Google users to post status updates or photographs, available to friends for view and comment in to 'Circles' which is primarily a group for multi-person instant messaging social networking system.

### 3.3.7. YouTube

YouTube is an American video-sharing website. It's allows user to upload, view, rate, share, add to playlist, report, comment on videos, and subscribe to other users. Most of the content on YouTube is uploaded by individuals. Unregistered user can only watch videos on the site, while registered users are permitted to upload an unlimited number of videos and add comment on videos.

## 3.4. Social Apps

Examples of popular Social apps are as follows:

### 3.4.1. WhatsApp Messenger

It is a freeware, cross-platform messaging and Voice over IP (VoIP) service owned by world famous and popular social media Facebook. It allows user to send text messages and voice messages, make voice and video calls, share images and documents, user location and others media. WhatsApp's client application run on mobile device, but it is also accessible from computer.

### 3.4.2. Google Maps

Google mapping service developed by Google. It's used by the individual for reached the location where we want to reach. While we use this Apps, we share our personal information to the google map. It explores our timeline by sending a mail. It explores how many distance covered by walk, how may time we spend in vehicle within a month, how may city and place we visited, it's also explored that, by which means we travel, etc.

### 3.4.3. Ola /Uber Apps

Ola cab is an Indian origin online transportation network company. The cabs are reserved through mobile apps or their website. It accepts both cash and cashless payments with Ola money. When we use this Apps, we share our personal information. address, email Id, credit card /debit cards detail, our locations, etc.

### 3.4.4. Aarogya Setu apps

Indian government launch an apps on April 2020, called Aarogya Setu to try and use data science to solve COVID-19 problem. This app is already wildly popular, having been downloaded over 20 million times.

Aarogya Setu is designed on the assumption that if two mobile phones are within Bluetooth range of each other's their owner are probably close enough to transmit the Corona virus. When two phones on which the apps have been installed come close to each other's, the apps get information about where the contact happened, with whom, and for what durations. If you subsequently test positive for the virus, details of all those you came in contact with over the past 30 days and who have a high likelihood of having been infected by you are sent to the Union Health Minister so that they can be tested on priority.

In this apps, user share all personally identifiable information submitted at the registrations as – Name, Age, Sex, Phone Number, etc. its apps also collect your location information history by GPS.

### 3.4.5. Zoom Cloud Meeting Apps

This is a cloud meeting app. Zoom has emerged as a leading teleconferencing provider during the COVID-19 pandemic. By this apps conduct meeting, online live class. Etc. In COVID-19 pandemic company, school, college, etc are closed. Then this apps are used by every company for the personal meeting, school, college, university use this apps for online live class.

This apps are created by user mail id and mobile number. In this apps everything from webcam or microphone security to sensitive datalike passwords, emails, or device information's are hacked by the hacker. There is no any protection for sensitive personal data.

### 3.5. Use of social media

Social media are a means of communication between the data subjects. They communicate to each other by online and create virtual communities using online social networks. A social network is a social graph which represents a relationship

among users, organizations, and their social activities. An online social network (OSN) is an online platform which are used by every user to create social networks or relationships with other people that have similar views, interests, activities, and/or real-life connections. A large number of different types of social-networking services are available in the current online space.[325]

The main goal of OSNs is to share data with maximum users. Users utilize OSNs, such as Facebook, Twitter, and LinkedIn, Ola, messenger, etc to publish their routine activities. Sometimes, OSN users share information about themselves and their lives with friends and college use. Typically, users share some parts of their daily life routine through status updates or the sharing of photographs and videos. Currently, various OSN users utilize smartphones to take pictures and make videos for sharing through OSNs. These data can have location information and some metadata embedded in it. OSN service providers collect a range of data about their users to offer personalized services, but it could be used for commercial purposes. In addition, users' data may also be provided to third parties, which lead to privacy leakages. This information can allow malicious users to leverage and invade the privacy of an individual

User generated content on social media may include data users' experiences, opinions, and knowledge, private data, for example, name, gender, location, and private photos. OSN users generally face the challenges of managing their social identity while compromising their social privacy.

Social-networking tools play a significant role in our social and business lives, at the same time they bring about high risks concerning privacy and security. Use of social media, online users have been exposed to privacy and security threats. These threats can be categorized into classic and modern threats. Classic threats are online threats that not only make OSN users vulnerable, but also other online users who do not use any OSN. The second type of threats is modern threats, which are related to OSN users only.

[325] Azhar Rauf "Privacy and Security Issues in Online Social Networks" 10 *MDPI* 2 (2018)

### 3.6. Use of Social Media and Data Privacy Threats

Present time we are use different type of social media. By use of these social media our data privacy is breach. Some modern threats are adversely affected to data privacy. These threats are typically related to Online Social Networking Sites (OSNs). Normally, the focus of modern threats is to obtain the private information of users and their friends. If users have their privacy setting on their Facebook account as public, they can be easily viewed. However, if they have the customized privacy setting, then it is viewable to their friends only. In this situation, the attacker can create a Facebook profile and send a friend request to targeted users. Upon acceptance of the friendship request, details are disclosed to the attacker. Fallowing modern threats are adversely affected the data privacy.

#### 3.6.1. Clickjacking

Clickjacking is also known as a user-interface redress attack, wherein a malicious technique is used to make online users click on something that is not the same for which they intend to click. In clickjacking attacks, an attacker can manipulate OSN users into posting spam posts on their timeline and asks for 'likes' to links unknowingly.[326]

#### 3.6.2. De-anonymization Attacks

De-anonymization is a strategy based on data-mining techniques, wherein unidentified information is cross-referenced with public and known data sources to reidentify an individual in the anonymous dataset. OSNs provide strong means of data sharing, content searching, and contacts. Since the data shared through OSNs are public by default, they are an easy target for deanonymization attacks[327]. In existing online services, pseudonyms are used for data anonymity to make the data publicly available.

#### 3.6.3 Fake Profiles

The fake-profile attack is also a problem for the OSN service providers because it misuses their bandwidth. A typical attack in most of the social networks is a fake-

[326] Azhar Rauf "Privacy and Security Issues in Online Social Networks" 10 *MDPI* 5 (2018)
[327] Azhar Rauf "Privacy and Security Issues in Online Social Networks" 10 *MDPI* 6 (2018)

profile attack. The goal of the fake profile is to collect the private information of users from the OSN, which is accessible only to friends, and spread it as a spam. In this kind of attack, an attacker creates an account with fake credentials on a social network and sends messages to legitimate users. After receiving friendship responses from users, it sends spam to them. Usually, fake profiles are automated or semiautomated and mimic a human. Moreover, it can be used for various purposes, for example, advertisements. Making fake followers and retweets is a large IT business, and it is possible because of fake profiles, but it gives misleading information to viewers.

### 3.6.4. Identity Clone Attacks

Profile cloning can be performed by an attacker using theft credentials from an already existing profile, creating a new fake profile while using stolen private information. The attacker can use the trust of the cloned user to collect contents from their peers or perform different types of online fraud.[328]

### 3.6.5. Information Leakage

Social media is a platform where all users are openly sharing and exchanging information with friends. Some users willingly share their personal information such as health-related data, genetic data[329] biometric data[330], demographic data[331], sensitive personal data[332] etc. Data hackers hack our all data and sold it on nominal price.

### 3.6.6. Location Leakage

The location-leakage threat is a type of data leakage. There is a trend for various users to access a social network through mobile devices. Usually, apps are used to access an online source through a mobile device. Google mapping service developed by Google. It's used by the individual for reached the location where we want to reach. While we use this Apps, we share our personal information to the google map. It explores our timeline by sending a mail. It explores how many distance covered by walk, how may time we spend in vehicle within a month, how may city and place we

[328] Lewis, J. How spies used Facebook to Steal NATO Chief's Details. The Telegraph, 2019
[329] Section 3 Clause (20) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[330] Section 3 Clause (8) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[331] Section 3 Clause (8) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[332] Section 3 Clause (35) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

visited, it's also explored that, by which means we travel, it's also explore that which place we stay, name of hotel, restaurant, etc. The use of mobile devices for online access introduces the new privacy threat of location leakage. The use of mobile devices for online access encourages users to share their location information. Thus, the revealing of geographic data on social-networking sites may be used by attackers to harm users.

### 3.7. Breach of Data Privacy by use of Social Media

Media is an effective instrument on communication, like a newspaper or a radio, so social media would be a social instrument of communication. Internet is now necessary part of life from shopping to electronic mails and education. It is a very large community, which is using internet for education, shopping, Entertainment, receive mails, share photos and video, etc. Internet is very big evolution of the technological era. The social media is "the relationships that exist between network of people". By social media, young men and women now exchange ideas, feelings, personal information, pictures and videos at a truly astonishing rate.

Our daily life we use SNSs and Social Media for our progressive life. In our daily life we share our personal data. When we use any welfare social scheme/ governmental plan or non-governmental plan, fill-up examinations form we share our Aadhaar Number, Email Id, Name, Address, Photo, signature, etc. when we show price of any items in the online shopping sites then we Shaw that that things ad see your mail, Facebook account, your Android phone etc. that means your personal data that you search on online shopping sites that are sale by online shopping sites to other sites, that is the breach of your data privacy. Withought your consent your personal data sell to others sites. When we use different social networking sites like. Facebook, Tweeter, Instagram, etc. we don't read the term and conditions of that Social Networking sites. That is big mistake by us, our all personal data have store on that sites. Our photo video massage, Email Id, etc are stored on that sites. They use that data for any purpose. When we use different Social media than we share our different personal data to that company.

We use Facebook's in our daily life for share information, photos, etc. Facebook's importance and scale has led to criticisms in many domains. Notable

issues include data privacy. Facebook is alleged to have psychological effects, including feeling of jealousy and stress, social media addiction. Facebook has been criticized for allowing user to publish illegal / offensive material. Specific include hate speech, incitement of rape, terrorism, crime murders, and livestreaming violent incidents.

In Sri Lanka, on 14 May 2019 Sri Lanka block social media Facebook and WhatsApp for maintain peace after worst anti-Muslim violence since Easter attacks.

The Facebook-Cambridge Analytica data scandal was a major political scandal in early 2018. In this scandal Cambridge Analytica had harvested the personal data of millions of people's Facebook profile withought their consent and used it for political advertising purpose. They shar our personal data without the consent of Data Principal, and breach their Data privacy.

We use online shopping sites like Amazon, Flip cart, Big basket, Paytm Mall, etc then our personal data store on that company. When we online ordered then our personal data, our address, Debit / credit card number, bank account, etc are share to that online shopping company. When we use Ola/ Uber for Traveling then we shar our current locations, last locations, credit/ debit card number, bank account etc. that's all of our personal data and sensitive data which we share to that Company.

When we use Google map in our Androids phone, then google map store our all activity. While we use this Apps, we share our personal information to the google map. It explores our timeline by sending a mail. It explores how many distance covered by walk, how may time we spend in vehicle within a month, how may city and place we visited, it's also explored that, by which means we travel, etc.

These different types of Social networking sites and different Social media Apps are breach our data privacy. These SNSs and Social Media have no any proper processing of data, and they don't safe our personal data. So, use of SNSs and Social media apps our data privacy breach.

### 3.8. Impact of Social Media on Different Fields

#### 3.8.1. Impact of social media on Educations

For the purpose of education social media has been used as an innovative way. In the educational classes' media just being used for messaging or texting rather than they should learn to figure out how to use these media for good.

Technology has shown a rapid development by introducing small communication devices and we can use these small communication devices for accessing social networks any time anywhere, as these gadgets include pocket computers, laptops, iPads and even simple mobile phones etc.[333]

Social media has increased the quality and rate of collaboration for students. With the help of social media students can easily communicate or share information quickly with each through various social sites like Facebook, Orkut, and Instagram etc. It is also important for students to do some practical work instead of doing paper work. Social networking sites also conduct online examination which play an important role to enhance the students' knowledge.[334]

##### 3.8.1.1. Positive Effect of Social Media on Education

- Social media gives a way to the students to effectively reach each other in regards to class ventures, bunch assignments or for help on homework assignments
- Teachers may post on social media about class activities, school events, homework assignments which will be very useful to them
- Many of the students who do not take an interest consistently in class might feel that they can express their thoughts easily on social media
- It is seen that social media marketing has been emerging in career option. Social media marketing prepares young workers to become successful marketers.

[333] Shabnoor Siddiqui and Tajinder Singh , "Social Media its Impact with Positive and Negative Aspects" International Journal of Computer Applications Technology and Research, Volume 5, Issue 2, p.g.71 - 75,
(2016).

[334] Supra Note 4

#### 3.8.1.2. Negative effect of Social Media on Education

- One of the biggest negative effects of social media in education is the privacy issues like posting personal information on online sites.
- By the use of Social Media many in appropriate information posted, which may lead the students to the wrong side.
- By the use of social media students lose their ability to engage themselves for face to face communication.
- Many of the bloggers and writers posts wrong information on social sites which leads the education system to failure.[335]

### 3.8.2. Impact of Social Media on Society

Many of the social media sites are most popular on the web. Some social media sites have transformed the way where people communicate and socialize on the web. Social networking sites render the opportunity for people to reconnect with their old friends, colleagues and mates. It also helps people to make new friends, share content, pictures, audios, videos amongst them. Social media also changes the life style of a society.

#### 3.8.2.1. Positive Effects of Social Media on Society

- Social media provides awareness among society like campaigns, advertisement articles, promotions which helps the society to be up to date with the current information.
- It also helps to share ideas beyond the geographical boundaries.
- Another positive effect of social networking site is its unite people on a huge platform for the achievement of specific goals. This brings positive change in the society.
- It provides open opportunity for all writers and bloggers to connect with their clients.
- Social Media helps to meet people they may not have met outside the social media forums.[336]

[335] Ibid

### 3.8.2.2. Negative Effects of Social Media on Society

- One of the negative effects of social media is that it makes people addicted. People spend lots of time in social networking sites which can divert the concentration and focus from the particular task.
- Social media can easily affect the kids, the reason is sometimes people shares photos, videos on media that contain violence and negative things which can affect the behavior of kids or teenagers.
- It also abuses the society by invading on people's privacy.
- Social lies like family ones also weaken as people spend more time connecting to new people.
- Some people use their images or videos in social sites that can encourage others to use it false fully.[337]

### 3.8.3. Impact of Social Media on Youngsters

Present time many young people's day to day life are woven by the social media. Youngsters are in conversation and communication with their friends and groups by using different media and devices every day. In past years it was seen that youngsters are in touch with only friends and their groups in schools and colleges. But nowadays youngsters are in contact not only with known friends but also with unknown people through social networking sites, instant messaging etc. Throughout the country teenagers frequently use the web, mobile phones, online games to communicate and gather information with each other.

### 3.8.3.1. Positive Effects of Social Media on Youngsters

- Social media helps youngsters to stay connected with each other.
- Useful information can be exchanged over social networking sites.
- Social networking sites can allow teens to find support online that they may lack in traditional relationships, especially for teens

[336] P. Krubhala and P. Niranjana, "Online Social Network - A Threat to Privacy and Security of Human Society" International Journal of Scientific and Research Publications, Volume 5, Issue 4, April (2015)
[337] Supra Note, 7

- In a Critical Development period youngster also go for social networking sites for advice and information.
- Youngsters can look to social media for getting the answers related to their career objectives.

#### 3.8.3.2. Negative Effects of Social Media on Youngsters

- Mostly youngsters waste lots of time on social sites like chatting which also effects their health.
- Kidnapping, murder, robbery can be easily done by sharing details on social media.
- There are many cases registered in police station where adults target young children and lure them into meeting them.
- Some useless blogs influence youth extremely that they become violent and can take some inappropriate actions.[338]

## 3.9. Impact of Social Networking sites on data privacy

There are many positive aspects of social networking, but there are equally as many dangers and negative aspects that come with the use of sites such as Facebook, Twitter, LinkedIn, Google+, Pinterest, Instagram, gaming sites, and blogs.

### 3.9.1. Positive Aspects

#### 3.9.1.1. In Education

In the educational field social media help by fallowing manner:

- Social media helps user for better collaboration and communication between teachers and students
- Social Media helps students, Researcher, Teachers, to Access online resources for learn, study, teaching, and research. its use for better and faster Research.

[338] Shabnoor Siddiqui and Tajinder Singh , "Social Media its Impact with Positive and Negative Aspects" International Journal of Computer Applications Technology and Research, Volume 5, Issue 2, p.g.71 - 75, (2016).

- By the use of Social Media Student improved grades along with reduced absenteeism in online sessions
- By the use of Social Networking Sites and Social Apps Student Teachers and researchers, all of them being discussed Educational topics and school assignments on social sites.

- **In Politics**

In the politics social media help by fallowing manner: -

- Increase in voter participation, seeing their friends voted on Facebook post
- More likely to attend a political meeting and rally seeing others on social sites
- Social movements have easy fast method of mobilizing people and sharing info

#### 3.9.1.2. For Awareness

For awareness of the people social media help by fallowing manner: -

- Information dissemination is faster than any media
- Breaking news spreads fast
- Access to previously inaccessible resources for academic research
- Helps inform and empower individuals to change themselves

#### 3.9.1.3. For Social Benefits

By the social media individual achieve fallowing benefits'

- Social media allow people to communicate with friends and this increased online communication strengthens those relationships, friendships
- People making new friends online.
- Helped find and keep in touch with friends who are geographically far off.

#### 3.9.1.4. For Job Opportunities

Social media also helpful for provide job opportunity,

- Great for marketing professionals
- Connect and find business opportunities

- Employers find candidates and unemployed find work faster
- Social media sites have created thousands of ecommerce jobs, new avenues.

### 3.9.2. Negative Aspects

#### 3.9.2.1. Apps access User Data

By the use of social media, Apps use the data of the data user by fallowing manner

- Social apps force users to grant access to their apps for list of things
- Access public profile information - user name, profile picture, friend list birthday, favourite movies and books, etc.
- Access posts in the News feed, Video and Photos posted;
- Post new message to the wall of the Facebook, without the consent of Facebook user
- Sending direct emails to the user email address
- Access family and relationships information

#### 3.9.2.2. Lack of Privacy

- By the use of social media
- Young people often give out personal information when online without reading the fine print privacy policies and unaware about misuse by third parties.
- Exposure to corporate and governmental intrusions
- Insurance companies use information gleaned from social media.
- Online advertising policies are an invasion of privacy. If clicked “like” for a brand, browser cookies give the company information and access about personal information and preferences.

#### 3.9.2.3. Users Vulnerable to Crime

- Unauthorized sharing of intellectual property can cause loss of potential income.
- Cyber-attacks like ransomware, hacking, identity theft and phishing are common problems faced by end users.

- Criminals browse social media to know user whereabouts and are known to commit crimes when away on vacation

#### 3.9.2.4. Waste of Time

Constant browsing and replying online posts and blogs, takes the user attention away from core work and often take some time to return to original task.

#### 3.9.2.5. Social Detriment

Cyber-bullying or use of electronic communication to bully someone by sending intimidating or threatening messages is commonplace online. This causes emotional trauma and sometimes even leads to suicide.

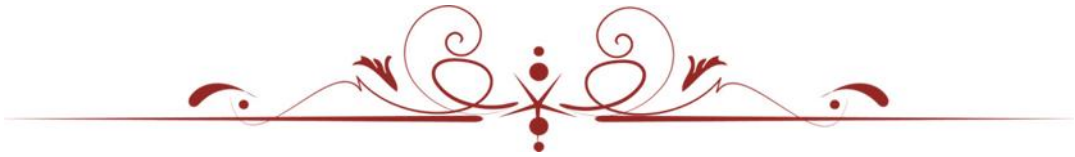
- Excessively being online correlated with personality and brain disorders
- Poor social skills and narcissistic tendencies or even need for instant pleasure with addictive behaviors and other emotional issues leading to depression, anxiety and loneliness.
- Less time for face-to-face interaction with loved ones.
- Youngsters are prone to feeling isolated, disconnected from real world and face higher risks of depression, low self-esteem and eating disorders

## 3.10. Conclusion

Present time we are living in Digital Era. Where everything is digital. Such as by e-library we do research on different fields, study books, magazine, articles, make their presentations, etc. by e-mail people send and received instant massage and information. By e-shopping people ordered daily use items, fashions items books, cloths etc. and received that items at their door step. By e-ticket people book their train ticket, Airplane ticket, movies ticket, museum and park ticket, etc. By e-payment people payment through Net Banking or mobile banking apps, when they purchase anything in anywhere. People use internet for travels and food orders, such as Ola, Uber, Swigi, Zomato, etc and share their personal data to the company. People use social media sites for Communications such as Facebook, Twitter. You Tube use for see and download video, and as well as uploads data in the internet. Internet has stored a massive amount of data or information and it is nothing but the Big Data.

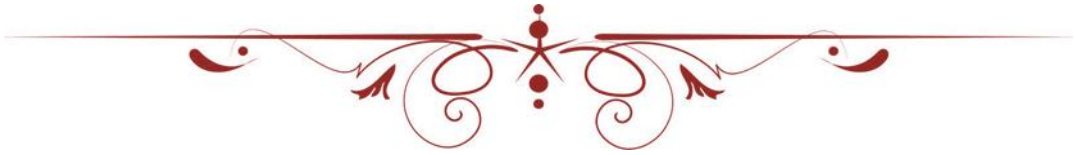
Dynamic nature of social media data is a significant challenge for continuously and speedily evolving social media sites.

When we use these SNSs and Social Media then we share a lot of personal data and sensitive personal data to that sites. These SNSs are store our data and share our data to others Social networking sites withought the consent of the data Principal. due to this reason Social networking sites are breach our data privacy. So, its required that Government draft a specific legislation for the protections of data privacy. Maximum people don’t know about data privacy so its required that aware people to their data privacy.



# Chapter IV

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



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

With the increased proliferation of technology in daily lives, it is becoming increasingly important for us to recognize and implement a Data protection law in India. In India there is no any specific legislation related to data privacy. In India issue related to the privacy dealt with the "Constitution of India", while issue related to the data Protection dealt with the "Information Technology Act,2000". Before the Puttaswamy Case there is no any specific legislation for protection of personal data. In the case of Puttaswamy Supreme Court given direction to the government for draft the data privacy protection law. This regards government constitute B.N. Krishna Committee for draft data protection law. 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. After the public comment and suggestion committee drat the "The Personal Data Protection Bill, 2018. Before this Bill, Shri Baijayant Panda introduce "The Data (Privacy and Protection) Bill, 2017 in Lok Sabha. Both these Bill are related to the data privacy, so it is necessary to analysis these Bill.

### 4.1. Analysis of The Data (Privacy and Protection) Bill, 2017

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 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 "The Data (Privacy and Protection) Bill, 2017" (Hereinafter say that "Bill of 2017") was draft by the BAIJAYANT PANDA in April 2017 before the judgement pronouncement in the case of Puttaswamy. This bill was specially introduced in Lok Sabha for the protection of data privacy. 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, Anonymised Data, Person, Authorised Officer, Data processing Data Controller, Data Processor, Third Party etc.

### 4.2. Objective of Bill

Objective of this bill to -

*"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"*[339]

It means there is two types of object given in this bill,

**(1)** To codify and safeguard the Right to Privacy in digital age,
**(2)** Constitute a Data Privacy Authority to protect the Personal Data

The first objective "To codify and safeguard the Right to Privacy in digital age" was given in this Bill because this Bill was introduced in Lok Sabha before the judgment of Puttaswamy Case. Before the Puttaswamy case Right to privacy is not a fundamental right, its dealt by the article 14, 19 and 21. So this objective is given in this Bill.

[339]The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

### 4.3. Extent of the Bill

"*It shall extend to the whole of India and, save as otherwise provided in this Act, it shall also apply to any offence or contravention thereunder committed outside India by any person*."[340]

It means this Bill was extent to whole territory of India. This Bill also apply outside India when the Offence or contravention thereunder the provision of this Bill.

### 4.4. Definitions

In this Bill defines some important words these are fallowing: -

**4.4.1. "Data"** means

*"for the purpose of this Act refer to data as defined under clause (o) of sub-section (1) of section 2 of the Information Technology Act, 2000"*[341]

It means the definition of Data as same meaning as define in Information Technology Act,2000.

This definition of data is very narrower than the definition of data in "The Personal Data Protection Bill, 2018".

**4.4.2.** "**Data Controller"** means

"*a person who, either alone or jointly or in combination with other persons, determines the purposes for which and the manner in which any personal data are used, or are to be, processed*"[342]

It means data controller is a person who determines that for which purpose and what is the manner to processing of personal data of an individual.

**4.4.3.** "**Data Processor"** means,

*"any person. apart from an employee of a data controller, who processes data independently or on behalf of a data controller"*[343]

[340] Section 1 Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[341] Section 2 Clause (f) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[342] Section 2 Clause (g) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

Data processor means any person who processes the personal data independently or on behalf of a data controller. But in data processor does not include the employee of data controller.

**4.4.4.** "**Person"** means,

"*for the purpose of this Act refer to an individual"*[344]

Word "Person" include only individual. It means only human being is the subject matter of data privacy. Legal persons are not the subject matter of the data privacy. It's exclude the Hindu undivided family and company.

**4.4.5. "Processing"** means,

*"Obtaining or recording the information or data or carrying out any operation or set of operations on the information or data, whether or not by automatic means, including-*

*(i) Organisation, Adaptation or Alteration of the information or data,*

*(ii) Retrieval, Consultation or use of the information or data,*

*(iii) Disclosure of the information or data by transmission, dissemination or otherwise making available, or*

*(iv) Alignment, Combination, Blocking, Erasure or Destruction of the information or data"*[345]

Processing means obtaining or record the data or information, whether it manually or automatic means. It is not necessary that it is obtaining or recorded by automatic means. The word processing also includes, *Organisation, Adaptation or Alteration Alignment, Combination, Blocking, Erasure or Destruction of the information or data*, etc.

**4.4.6. "Surveillance"** means

*"any activity intended to collect, watch, monitor, intercept, or enhance the ability to do the same with a view to obtain information about a person, group*

[343] Section 2 Clause (h) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[344] Section 2 Clause (k) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[345] Section 2 Clause (n) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

*of persons or class of persons through analysis of any communication, images, signals, data, movement, behaviour or actions"*[346]

The word "Surveillance" define in the Bill of 2017, but it does not define in the Bill of 2018. In simple word surveillance means "Keep an eye on". Surveillance is an activity to collect or obtain information about a person, or group of a person.

**4.4.7. "Sensitive Personal Data"** means,

*"Such personal information which consists of information relating to—*

*(i) Medical records and history*

*(ii) Financial information such as bank account or credit card or debit card or other payment instrument details or financial transactions records;*

*(iii) Passwords*

*(iv) Sexual activity*

*(v) Physical, Physiological and Mental health condition;*

*(vi) Racial or Ethnic origins, Political or Religious views;*

*(vii) Biometric data relating to the physical, physiological or Behavioural characteristics of a natural person"*[347]

In simple word "Sensitive personal data" means personal data which is required more privacy. A personal data which is required more privacy and protection than a personal data it is a Sensitive personal data, as -Bank Account, ATM PIN, Email password, Sexual activity, Health records, Biometric data, Political or Religious view, Physical or Mental health condition, etc. all are covered within the sensitive personal data.

**4.4.8. "Profiling"** means,

*"any form of automated processing of personal data consisting of the use of personal data or to record and classify behaviour of individuals to predict and analysis their daily activities for purposes other than promotion and marketing of goods and services"*[348]

[346] Section 2 Clause (r) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[347] Section 2 Clause (s) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[348] Section 2 Clause (q) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

Profiling is an automated processing of personal data. It is use for the predict and analyzed the daily activity of individuals. In the profiling "Recording and analysis of a person's psychological and Behavioural Characteristic, so as to access or predict their capabilities in a certain sphere or assist to identifying categories of people.

### 4.5. Applicability of this Bill[349]

This act shall apply to,

*"collection, use, storage, disclosure and processing of personal data or information of all persons through wholly or partially automated or manual methods"*

It is applicable where collection, use, Storage, Discloser and processing of personal data of all persons through wholly or partially automated or manually.

This Bill also apply to,

"*Data controllers and data processors which are State entities, including Government agencies or authorized personnel on their behalf as well as private companies, partnerships or any other body corporate which conduct activities……*[350].

This Bill also applicable to data controller and data processor which are State Entities. Data processor and data controller also include the Government agencies, Authorized personnel, or on their behalf as well as private companies, partnerships firm or any other body corporate which conduct activities within the territory of India through a registered place of business.

### 4.6. Non-Applicability of this Bill

This bill does not apply to the collection or processing of data which is mentation in Schedule I.

"*Nothing in this Act shall apply to collection or processing of data mentioned in Schedule I.*"[351]

[349] Section 3 Clause (1) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[350] Section 3 Clause (1)(b) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[351] Section 3 Clause (1) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

It means, this Act shall not apply to collection or processing of data which falls within the following categories—

**1.** Purely for personal reasons or pertaining to household activities;

**2.** Of a deceased person;

**3.** Eligible to be disclosed under the Right to Information Act, 2005; and

**4.** Anonymised data and cannot be used to identify the natural person.

Schedule I is amend by the central government. According proviso of section 3 (2) of the Data (Privacy and Protection) Bill,2017, central government have power to amend the Schedule I, by notification in the Official Gazette. Every notification of the amendment of Schedule I, is issued after consultation with the Authority and shall be led before the House of Parliament.

### 4.7. Right to Privacy and Data Protection

Chapter II of this Bill dealt the Right to Privacy and Data Protection. Section 4 dealt the right to privacy. The title of section 4 is "Right to Privacy". In section 4 fallowing provision is mentation,

"*Notwithstanding anything contained in any other law for the time being in force, pursuant to article 19 and 21 of the Constitution and subject to the provisions of this Act, all persons shall have a right to privacy"*[352]

It means all person have right to privacy, but this right is subject to provision of this Act. Present time the value of section 4 is nothing because this bill was draft before the judgement of Puttaswamy case, and that time right to privacy is not a fundamental right, but present time right to privacy is a fundamental right. So, the value of section 4 is nothing at present scenario.

Ever person have right to data privacy. But this is not absolute right, it is a qualified right. Section 15 of this Bill led down restriction on this right,

[352] Section 4 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

*"Notwithstanding anything contained in this Act, the right to privacy shall be restricted by the Authority in the manner specified by this Act*"[353]

Restriction on this right is led down by the data privacy authority in that manner which is specified by this act. But it is required that the restriction must be adequate, relevant, proportionate, not extensive in nature and must be imposed in the manner prescribed. Restriction impose on the right to privacy for the fallowing reason that is,

a) Safeguards for sovereignty or integrity of India, National Security of Country
b) Prevention from terrorism, money laundering, corruption, organized crime
c) Maintenance of public order in situations of imminent danger of breakdown
d) Investigation of cognizable and non- cognizable offence under the Indian Penal Code, 1860[354]

These are the restriction on the right to privacy.

### 4.8. Right to Secure Personal Data

Every person has right to secure his personal data. Any person has no right to collect, store, process, discloser, or handle personal data of other persons. If any person wants to collecting, disclosing, processing, storing personal data of another person, then it is required that express and affirmative consent has to be obtained from the requisite person. When consent is freely given then it deemed valid consent otherwise invalid consent.[355] According to section 16 of this Bill "Consent should be express, affirmative and taken after information as mandate under Schedule II."[356] When consent obtain from any person this is the duty of data controller or data processer to dully provide information and adequate explanation to the person that which extent his personal data shall be accessed, collected, stored or processed. The word "Consent have the same meaning as provided under the Indian Contract Act,1872.

[353] Section 15 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[354] *Ibid.*
[355] Section 5 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[356] Section 16 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

When the personal data is belonging to the minor, the consent of minor shall be obtaining from a legal guardian and dully verified by the data controller and data processer.[357] When the minor attaining the majority minor have the right to either continue or terminate the consent given by the legal guardian on his behalf of.

When any person gives his consent for collection, processing, use or storage his personal data shall be have a legitimate expectation that data controller and data processers abide by the provision of this Act[358]. It is the duty of data controller and data processer shall take all security measures necessary for safeguarding and securing the personal data in their custody with due diligence[359]. This obligation given to data controller and data processer by the security Protocol[360]. This security Protocol is notified by the Central Government with the prior consultation with the data protection authority.

### 4.9. Right to Accessed Personal Data

Every person has right to access his /her personal data. This right is given in section 8 of the Bill of 2017. According to this section every person has the right to access his personal data which is collected, processed use or stored by Data controller and Data processor. This right also include the right to obtain a copy and obtain confirmation that his data is being processed along with any supplementary information.[361]

### 4.10. Right to Rectification of Personal Data

When the personal data of any person is inaccurate or incomplete then person have right to rectified his personal data by the data controller or data processer. This right is given in section 9 of the Bill of 2017. According to this section,

*"Every person shall have the right to have his personal data rectified if it is inaccurate or incomplete"*[362]

[357] Section 17 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[358] Section 14 Clause (1) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[359] Section 14 Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[360] Section 28 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[361] Section 8 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[362] Section 9 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

Means every person have right to rectified his personal data if his personal data is incomplete or inaccurate. Rectification is carried out by the data controller or data processer in that manner which is rectified by the Central Government with the consultation by the Data Protection Authority. It is note that every rectification shall be complete within a period of sixty days from the receipt of data for rectification.[363]

### 4.11. Right to Removal of Personal Data

Every personal data is collected or storage a specific purpose, when this specific purpose is fulfilled and data is no longer necessary then the data subject have right to seeking removal of personal data. This right is given in section 10 of the Bill of 2017. According to section 10 of the Bill of 2017,

*"Every person shall have the right to seek removal of personal data from Data Controller"*[364]

It means every person whose personal data is storage, process, have right to removal of personal data. Right to removal means "Right to delete his personal data". Removal of our personal data by the data controller on the fallowing ground, that is

**(a)** Where personal data is no longer necessary and purpose of data collection is fulfilled
**(b)** Where the person withdraws consent
**(c)** Where personal data obtain unlawfully
**(d)** Where personal data is required to be erased in accordance with legal obligation pursuant to a court order.[365]

This right is not absolute.it is qualified right. It means some restriction on this right. This restriction is led down in section 10 (2) of the Bill of 2017. According to this section, removal of personal data shall not be allowed on the fallowing ground, that is

If there are overriding legitimate interest and it is necessary-

[363] Section 9 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[364] Section 10 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[365] *Ibid*.

**(a)** in the interest of fundamental rights;

**(b)** for compliance of a legal obligation or court order or an any action taken by an officer in exercise of the power vested in him

**(c)** for establishing or defending a legal claim;

**(d)** to safeguard public interest.[366]

### 4.12. Transfer, Storage, and Security 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.

#### 4.12.1. Prohibition on Unnecessary Storage of Personal Data

Personal data collect, storage or processes for specific purpose, when the said purpose is achieved the it is required that destroyed the personal.

According to section 23

*"No person shall store any personal data of another person for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation."*[367]

*Any person shall not* store personal data of other persons for a period longer than necessary to achieve the purpose for which it was collect or received. When the purpose is achieved or cease to exit for any reason then it is required that personal data be destroyed forthwith.[368] But some circumstances personal data is retaining longer time they don't destroyed, that circumstance is provide fallowing, that is

**a)** Historical
**b)** Statistical or

[366] Section 10 Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[367] Section 23 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[368] Section 23 Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

**c)** Research purpose[369]

On the above mentation ground personal data cannot destroyed while the purpose of the storage of personal data is achieved.

### 4.13. Obligation of Data Controller and Processers

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.

#### 4.13.1. Collection of Personal Data in Fair and Lawful Manner

It is the responsibility of data controller and data processer to collect, storage, processes, the personal data in a fair, lawful, and transparent manner and compliance the provision of this Act.[370] When the personal data is obtaining and not fulfill the prescribe provision of this Act, it shall be deemed to be it is unlawfully obtained.[371]

#### 4.13.2. To Maintain Confidentiality of Personal Data

It is the duty of the of the data controller, data processor or third part, as the case may be

(a) to ensure that all personal data is reasonably shared when necessary
(b) maintaining confidentiality and compliance the provision of this Act[372]

#### 4.13.3. Fortification of data security

"Fortification" means "to act of strengthening something". In informational privacy it is used for data security. By the fortification of data security, protected from the unlawful access or use of data, accidental loss, damage, or cyber-attack. It is the duty of the data controller or processer or third party to take adequate measure for fortification of data security. When the data security and breach of data privacy of an

[369] Section 23 Clause (2) (b) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[370] Section 29 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[371] Section 29Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[372] Section 30 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

individual then it is the duty of data controller or processer or third party to notify the affected person within seven days of the occurrence of the breach of data privacy[373].

### 4.13.4. Appointment of Data Protection Officer[374]

Data protection officer is the technical expert in field of data security. Data Protection Officer (DPO) is appoint by the data controller or data processer or third party. Data protection Officer having adequate technical expertise in the field of data collection or processing. Data protection officer have ability to address any request, clarifications or complaints made with regards to the provision of this Act.

## 4.14. Data Privacy Authority

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.

### 4.14.1. Constitution of Data Privacy Authority[375]

Data Privacy and Protection Authority constitute by the central Government by notification in the official Gazette. Constitute of the authority for carrying out the purpose of this Act in such a manner as may be prescribed.

### 4.14.2. Power and Procedure of the Authority

Authority is not bound by the procedure laid down by the code of Civil Procedure,1908.[376] Authority regulate its own procedure[377]. It means authority have discretionary power to regulate his own procedure. This discretionary power is not absolute. It is guided by the

(a) principal of natural justice, and
(b) subject to the other provision of this Act[378]

[373] Section 31 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[374] Section 34 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[375] Section 44 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[376] Section 48 Clause (1) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[377] Section 48 Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[378] Section 48 Clause (1) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

For the discharging his function by the authority under this Act, authority have the same power as are vested in the Civil Court under the Code of Civil Procedure, 1908[379]. Which is namely:

(a) requiring the discovery and production of documents or other electronic records;

(b) summoning and enforcing the attendance of any person and examining him on oath

(c) issuing commissions for the examination of witnesses or documents

(d) receiving evidence on affidavits:

(e) calling upon any data processor or data controller at any time to furnish in writing such information or explanation as may be deemed necessary;

(f) dismissing an application for default or deciding it ex party

(g) reviewing its decisions[380]

### 4.14.3. Constitution of Bench

Constitution of the bench by the data privacy and protection authority. Bench is constituted by notification in the official Gazette. Bench is constituted for the fallowing purpose, that is

"to exercise the jurisdiction, power and authority confirm by this Act"[381]

Bench is constituted by at least one judicial member and at least one technical member. It is the minimum requirement of the constitution of bench.[382]

### 4.14.4. Function of the Bench

Regarding this Bill, function of the bench is fallowing provided that is,

(a) Adjudicate all disputes and contraventions of the provisions of this Act referred to it,

[379] Section 48 Clause (3) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[380] Section 48 Clause (3) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[381] Section 46 Clause (1) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[382] Section 46 Clause (2) of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

(b) Impose penalties and punishments

(c) Consult with stakeholders on any issues pertaining to the subject matter of this Act which are of public importance;

(d) Consult with the Central Government according to the provisions of this Act

(e) Suo-moto initiate inspection of Data Controllers and Data Processors to assess compliance with the provisions of this Act.[383]

### 4.14.5. Filing of Complaints[384] and its Appeal[385]

Any person aggrieved by the decision of the data protection officer may file a written complaint before the Authority. This written complaint regard to non-compliance, contravention or any other violation of this Act. In this Bill adjudication power given to the Authority. When any complaint put down before the authority, the authority adjudicates the complaints and award fine, compensation, imprisonment of such term as it may be deemed appropriate[386].

If any person aggrieved by the decision of the bench then aggrieved person has right to appeal before the Telecom Disputes Settlement Appellate Tribunal. This Tribunal is set up in accordance with the provision of Telecom Regulatory Authority Act,1997.

Any suit or proceeding which is fall within the ambit of this Bill, there is no jurisdiction of Civil Court to entertain these matters.[387]

## 4.15. Offences and Penalties

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.

---

[383] Section 49 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[384] Section 50 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[385] Section 52 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[386] Section 51 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[387] Section 53 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).

Every offences under this Act treated as Cognizable offence[388]. 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[389].

Where these offences related to the sensitive personal data then the term of punishment for which may extent up to ten years imprisonment and fine which may extend up to rupees one lakh for each day of unlawful access to the sensitive personal data.[390]

When any person non-compliance of a direction or order of the bench then he punished with imprisonment for a term which may extend up to six month and fine which may extend up to rupees fifty thousand for each day of said breach.[391]

### 4.16. Analysis of the "The Personal Data Protection Bill, 2018"

The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy. Instrumentally, a firm legal framework for data protection is the foundation on which data driven innovation and entrepreneurship can flourish in India. Fostering such innovation and entrepreneurship is essential if India is to lead its citizens and the world into a digital future committed to empowerment, experiment and equal access.

In the case of Justice **K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others**[392]

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*

[388] Section 59 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[389] Section 54 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[390] Section 55 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[391] Section 58 of The Data (Privacy and Protection) Bill,2017 (Bill No.100 of 2017).
[392] W.P. NO. 494 of 2012

*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."*[393]

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.[394]

[393] https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf
[394] Suneeth Katarki, "The Personal Data Protection Bill, 2018 Key Features and Implications" *Indus law (August 2018).*

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".

### 4.17. Purpose of the Bill

According to this Bill Right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy. So the first purpose of this bill is "to protect personal data" which is essential facet of informational privacy.

It is necessary to create a collective culture that fosters a free and fair digital economy respect to the informational privacy of the individuals and ensuring empowerment, progress and innovation.

The third purpose of this Bill is expedient to make provision,

(a) to protect the autonomy of individuals in relation with their personal data
(b) to lay down norms for cross-border transfer of personal data
(c) to specify the rights of individuals whose personal data are processed
(d) to specify where the flow and usage of personal data is appropriate
(e) to create a framework for implementing organizational and technical measures in processing personal data
(f) to create a relationship of trust between persons and entities processing their personal data
(g) to ensure the accountability of entities processing personal data, to provide remedies for unauthorized and harmful processing
(h) to establish a Data Protection Authority for overseeing processing activities[395]

This bill is extent to the whole of India. It means it is also applicable in Jammu and Kashmir.

[395] The personal Data Protection Bill,2018.

### 4.18. Applicability of the Bill

This bill has adopted the intra-territorial and extra-territorial jurisdiction. Section 2 Clause (1) of this Bill dealt the intra-territorial jurisdiction, while Section 2 Clause (2) dealt the extra-territorial jurisdiction. According to section 2 clause (1) of this Bill,

*(a) processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; and*

*(b) processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law*[396].

It means this Bill shall be applicable to processing of personal data:

(i) where personal data has been collected, disclosed, shared or processed in any manner within the Indian territory; and

(j) (ii) where the processing has been undertaken by the government, by any Indian company, by any Indian citizen or any person or body of persons that has been incorporated under the Indian laws.

So, the Bill recognizes the principle of territoriality and nationality in defining the scope of application.

According to Section 2 Clause (2) of this Bill, Act shall apply to the processing of personal data by data fiduciaries[397] or data processors[398] not present within the territory of India, only if such processing is —

*(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or*

*(b) in connection with any activity which involves profiling of data principals within the territory of India*.[399]

[396] Section 2 Clause (1) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[397] Section 3 Clause (13) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[398] Section 3 Clause (15) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[399] Section 2 Clause (2) of "The Personal Data Protection Bill, 2018 (Bill of 2018).

It means, the Bill shall also be applicable to where data processing undertaken by a data fiduciary or data processor not located within the territory of India, if such processing is

(i) in connection with any business that is carried out in India or

(j) if the there is any systematic activity[400] of offering goods and services to data principals within the territory of India or

(ii) in connection with any activity that involves profiling of data principals within the territory of India.

### 4.19. Non-Applicability of this Bill

According to section 2(3) of the Bill,

*"Notwithstanding anything contained in sub-sections (1) and (2), the Act shall not apply to processing of Anonymized data"*[401]

It means this bill shall not apply to Anonymized data.[402]

### 4.20. Definitions

**4.20.1. Adjudicating Officer** means,

*"an officer of the adjudication wing under section 68[403]"*

In general sense "Adjudicating Officer" means an officer who have power to adjudicate the data privacy matter. According to above mention definition adjudicating officer means an officer of adjudicating wing which is appoint according the provision of section 68 of this Bill.

According to 68 of this Bill adjudicating officer is appoint by the central Government. Adjudicating officer must have special knowledge of, and not less than seven years professionals experience in the field of constitutional law, cyber and Internet laws, Information Technology law, Data protection and related subject.[404]

[400] Section 3 Clause (40) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[401] Section 2 Clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[402] Section 3 Clause (4) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[403] Section 3 Clause (2) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[404] Section 68 of "The Personal Data Protection Bill, 2018 (Bill of 2018).

**4.20.2.** "**Authority"** means,

*"Data Protection Authority of India established under Chapter X of this Act"*[405]

Authority means Data Protection Authority of India which is appoint under Chapter X of this Act. According to section 49, Central Government have power to stablish the authority by notification for the purpose of this Act[406]. The authority shall consist of seven members, one chairperson and six whole time members[407]. The chairperson and the member of the authority shall be appointed by the central government on recommendation made by a selection committee[408].

**4.20.3. "Anonymisation"** means, in relation to personal data,

*"the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority.*[409]*"*

Anonymization refers to the process of removing identifiers from personal data in a manner ensuring that the risk of identification is negligible. Anonymization requires the use of mathematical and technical methods to distort data to irreversibly ensure that identification is not possible[410]. It is an irreversible process of transforming or converting personal data to a form in which data principal cannot be identified.

**4.20.4.** "Anonymised Data" means,

*"data which has undergone the process of anonymisation under sub-clause (3) of this section"*

Anonymized data means data which has undergone the process of anonymization. Data anonymization is a type of information sanitization whose intent

[405] Section 3 Clause (6) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[406] Section 49 Clause (1) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[407] Section 50 Clause (1) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[408] Section 50 Clause (2) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[409] Section 3 Clause (3) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[410] B.N Krishna Committee Report on "Data Protection in India" (July, 2018).

is privacy protection. In anonymized data the data is converting or transforming to another form in which data principal cannot be identified.

**4.20.5.** "**Data"** means and includes,

"representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means[411]"

The terms "information" and "data" are the two different word in the context of informational privacy and data protection. It appears that the word data is of comparatively more recent origin than the word information. It is used in specialized scientific fields. The word has specific connotations in the fields of computer science and information technology. 'Information' on the other hand simply means facts about something or someone[412].

The word "Data" also include

(a) representation of information,
(b) facts,
(c) concepts,
(d) opinions,
(e) interpretation,

we use the term data as the broader term which includes any form of information. It is clear that data can be facts, objective information or even opinions or any other sort of information. It is wider than information. Data also include the information.

**4.20.6.** "**Personal Data**" means,

*"data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature*

[411] Section 3 Clause (12) of "The Personal Data Protection Bill, 2018 (Bill of 2018).
[412] B.N Krishna Committee Report on "Data Protection in India" (July, 2018).

*of the identity of such natural person, or any combination of such features, or any combination of such features with any other information"*[413]

The objective of this bill is to "to protect the personal data". So it is necessary to define the personal data. The definition of personal data is the critical element which determines the zone of informational privacy. The object of defining personal data is to demarcate facts, details or opinions that bear a relation to his or her identity.[414]

Personal Data is relating to a natural person. Person is directly or indirectly identifiable by any characteristic, trait, attribute, or` any other feature of the identity. These characteristic, trait, attribute, or feature of identity are personal data of a individual. Personal data is given information about the individual.

**4.20.7. Sensitive Personal Data**[415]" means

*"personal data revealing, related to, or constituting, as may be applicable—*

*(i) financial data; (ii) passwords; (iii) health data*[416] *(iv) caste or tribe (v) religious or political belief or affiliation (vi) sexual orientation (vii) biometric data*[417] *(viii) genetic data*[418] *(ix) transgender status*[419] *(x) intersex status*[420] *(xi) official identifier (xii) sex life (xiii) any other category of data specified by the Authority under section 22*

There has been no clear-cut approach towards categorizing sensitive personal data. In a contextual approach, i.e., where any personal data can become sensitive depending on the circumstances and the manner in which it is being processed.

However, this approach may place significant burden on data fiduciaries and regulatory resources as they would have to determine whether the personal data in

[413] Section 3 Clause (29) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[414] B.N. Krishna Committee Report on "White Paper of the Committee of Experts on A Data Protection Framework for India" (January 2018).
[415] Section 3 Clause (35) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[416] Section 3 Clause (22) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[417] Section 3 Clause (8) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[418] Section 3 Clause (20) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[419] Section 3 Clause (41) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[420] Section 3 Clause (23) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

question is sensitive or not, and whether it is capable of causing great harm to the individual, on a case by case basis.[421]

Data sensitivity, in one view, can depend on the legal and sociological context of a country. However, certain categories of personal data are capable of giving rise to privacy harms regardless of context and an objective method of identifying such kinds of data becomes necessary.[422]

According to "*any other category of data specified by the Authority under section 22"*

we have prescribed the following criteria to categories what is sensitive

(i) any expectation of confidentiality that might be applicable to that category of personal data

(ii) whether a significantly discernible class of data principals could suffer harm of a similar or relatable nature;
(iii the likelihood that processing of a category of personal data would cause significant harm to the data principal
(iv) the adequacy of general rules to personal data.

Based on the above criteria, categories the following as sensitive personal data in this Bill.

(a) Health data (b) Financial data (c) Official identifiers which would include government issued identity cards (d) Passwords (e) Sex life and sexual orientation (f) Caste or tribe (g) Religious or political beliefs or affiliations (h) Biometric and genetic data (i) Transgender status or intersex status.

Processing of these types of data can result in greater harm to the individual. Consequently, processing of these types of data will require stricter rules or grounds in law to minimize such harm.

[421] B.N Krishna Committee Report on "Data Protection in India" (July, 2018).
[422] Ibid.

**4.20.8. "Genetic Data"** means,

*"personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question"*[423]

Genetic data means, personal data of a natural person which is related to the inherited or acquired genetic character. Genetic data give us unique information about the behavioral characteristic, physiology or health of that natural person. It is obtaining by analysis of biological sample of natural person. It is a Sensitive personal data, so it is required more privacy for genetic data.

**4.20.9. "Biometric Data"** means,

*"facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person"*[424]

Definition of Biometric data is same, as define in General Data Protection Regulation 2018, (GDPR)

Biometric Data is similar to personal data which is resulting from measurement or technical processing operations carried out on physical, physiological or behavioral characteristic of a data principal. This biometric data is allowed or confirm the unique identification of that natural person.

Biometric data is a general term used to refer to any computer data that is created during a biometric process. This include samples, models, finger prints, similarity scores and all verification or identification data excluding the individuals name and demographics.

Biometric data can be used for all kinds of reason: finger print scanning to unlock you phone, fascial recognition software to improve your security system.

[423] Section 3 Clause (20) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[424] Section 3 Clause (8) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

Biometrics is the science of analyzing physical or behavioral characteristics specific to each individual in order to be able to authenticate their identity. If we were defined the biometrics in simple sense we would say the **"Measurement of the human body".** There are two types of measurement,

(1) Physiological measurements
(2) Behavioral measurements

In Physiological measurements their can, be either morphological or biological. These meanly consist of fingerprints, the shape of the head, iris and retina shape of the face for morphological analyses. For biological analyses, DNA, blood, urine may be used by medical teams and police forensics.

In behavioral measurement most common are voice recognition, signature, keystroke dynamic, gesture, etc

Biometric data can be used for all kinds of reason: finger print scanning to unlock you phone, fascial recognition software to improve your security system.

**4.20.10.** "**Person**" means,

"(i) an individual (ii) a Hindu undivided family (iii) a company (iv) a firm (v) an association of persons or a body of individuals, whether incorporated or not, (vi) the State (vii) every artificial juridical person, not falling within any of the preceding subclauses"[425]

The definition of the "person" in this Bill is wider than definition of "person" is given in "the data (Privacy and Protection) Bill,2017. In the bill of 2017, person means only Individual. while in the Bill of 2018, person include the, individual a Hindu undivided Family, a company, a firm, the State, artificial juridical persons, etc. It means every entity which is include in person, have right to data protection.

**4.20.11.** "**Data Principal**" means,

"the natural person to whom the personal data referred to in subclause (28) relates"[426]

[425] Section 3 Clause (28) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[426] Section 3 Clause (14) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

It means data principal is a natural person. whose personal data is collect, storage, processes, by data controller or data processer. Data principal is the core subject of data protection. In the personal data protection act, 2010 (DPA) the word "Data Subject" are used which is similar to Data Principal. According to DPA Data subject is an individual who is the subject of personal data.[427] But in according to this bill the word "Data Principal" is wider than "Data Subject" because in the section 3(28) the word "Person" define Which include the individual, a Hindu undivided family, a company, state, etc. while the "Data subject" include only individual. Data principal is the focal actor of digital economy.

**4.20.12. "Data Fiduciary"** means,

*"any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data"*[428]

Word "Data fiduciary" is includes

(a) Any person
(b) State
(c) Company
(d) Any Juristic entity
(e) Any individual who alone or conjunction with others

Duty of the Data Fiduciary to Determine the purpose and means of processing of personal data. It means data fiduciary is determine that for what purpose our personal data is processing, and by which means it is processing. This is the duty of the data fiduciary to determine that the processing done in fair and reasonable.

**4.20.13.** "**Data Processer**" means,

*"any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary"*

[427] Section 4 of the "Personal Data Protection Act,2010" (Act of 2010).
[428] Section 3 Clause (13) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

In generally a data processer is person who process data on behalf of a data fiduciary. Data fiduciary to decide the purpose and manner to be fallowed to process the data. Data processer hold and processes data but do not have any responsibility or control over that. It means data processer is any person who processes the personal data of the any person. Data processer also include the,

(a) State
(b) Company
(c) Any juristic person

But it does not include an employee of data fiduciary.

According to PDP Act 2010, data processer means,

"Any person other than employee of data user, who processes the personal data solely on behalf of the data user and does not processes the personal data for any of his own purposes."[429]

**4.20.14. "Processing"** means,

*"in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction"*[430]

In this Bill, Processing is always related to the processing of personal data. In generally, data processing is "the collection and manipulation of items of data to produce meaningful information."

Processing is an operation or set of operations performed on personal data. It's also included the, collection, recording, storage, adaption, alteration, use, retrieval, indexing, discloser by transmission, destruction, etc. Similar definition is given in Section 4 of the PDP Act,2010. The definition under the PDPA is wider in the sense that merely being in possession of personal data will be consider as processing.

[429] Section 4 of the Personal Data Protection Act,2010 (Act of 2010).
[430] Section 3 Clause (32) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

**4.20.15. "De-identification**" means,

*"the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal"*[431]

De-identification is the re-processes of personal data, which is storage have data fiduciary or data processor. By the de-identification process data fiduciary or data processer may remove, or mask identifier from personal data. In de-identification processes personal data replace with such other fictious name or code which is unique to an Individual. Through this unique code data principal identify directly.

## 4.21. DATA PROTECTION OBLIGATIONS

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.[432] 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. So the fallow these principles very carefully, unless a relevant exemption applies.

Section 5(1) of the PDPA, state that,

*"a data user must comply with all the data principles as set out…"*[433]

The word "must comply" indicate that, these principles shall fallow by the data user. If the data user not fallow these principles, shall be liable for punishment or fine or both.

These data protection principles are inserted In the chapter II of the "The Personal Data Protection Bill,2018". Section 4 to 11 of this bill dealt these data protection

[431] Section 3 Clause (16) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[432] David Bainbridge, Data Protection Law 60 (Universal Law Publication, Delhi,2nd edn.,2007).
[433] Section 5(1) of the Personal Data Protection Act,2010 (Act of 2010).

principles. According to chapter II of this Bill, some obligation of that person who processing our personal data, to fallow the fallowing data protection principal, these are,

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

Similar data protection principal is given to the Schedule I of the data Protection Act,1998. Now One by one analyzed these principles.

### 4.21.1. Fair and Reasonable Processing

This principle is provided in Section 4 of the Bill of 2018. Fallowing provisions are provided in Section 4 for the fair and reasonable processing,

*"Any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal."*[434]

According to section 4 of this Bill, any person who processes personal data of the data principal, it is the duty of that person, to process such personal data in a fair and reasonable manner and fallow the privacy of data principals.

The obligation to process fairly implies that the data fiduciary must act in a manner that upholds the best interest of the privacy of the principles. Further, the obligation to process reasonably also implies that the processing must be of such a nature that it would not go beyond the reasonable expectations of the data principal. Ensuring fairness and reasonableness in processing are obligations that go beyond simply lawful processing on the basis of one of the grounds laid down in law.[435]

[434] Section 4 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[435] B.N Krishna Committee Report on "Data Protection in India" 52 (July, 2018).

In determining whether processing is fair, regard is to be had to be method by which the data are obtain. If the data obtain by lawful means then it fair obtains, if it is obtaining by unlawful means then it is unfair obtain. If personal data are obtained from either the data principal another person by means of unlawful trick then the processing will be unfair. Fair processing should also have required that the data subject is informed of any non-obvious use to which the data controller intends to put the data at the time the data are collected. When data obtain from a person who was authorized by or under any enactment to supply such data are treated as fairly obtain.[436]

In determine the weather processing is reasonable or not, this regard to see the data processer is fallow all data privacy principal or not. If data processer fallows all data privacy principles then deemed that data processing is reasonable otherwise not reasonable.

So, its required that the processing of data should be fair and reasonable.

### 4.21.2. Purpose limitation Principle

Purpose limitation principal is provided in section 5 of this Bill. In section 5, provided following provision related to the purpose limitation principles,

*"Personal data shall be processed only for purposes that are clear, specific and lawful"*[437]

It means processing of personal data only for the any legal purpose. Purpose should be clear, specific and lawful. Purpose of processing should be clear. There is no ambiguity, the purpose should be clear.

The purpose limitation principle has been the bedrock of data protection regimes for the last three decades. It contains two sub-principles: first, that the purpose for which the personal data is processed must be clearly specified to the data principal. This is calling the "purpose specification." second, the processing must be limited to such purposes, or other compatible purposes. This is calling the "use limitation". Implicit in each of these sub-principles are two assumptions: first, that

[436] David Bainbridge, Data Protection Law 62 (Universal Law Publication, Delhi,2nd edn.,2007).
[437] Section 5 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

specification of purpose must meet a certain standard of specificity, simply specifying purposes in a vague manner will not be sufficient. Second, any unspecified use will be determined from the point of view of whether the processing is fair and reasonable in light of the purpose that was specified.[438]

The purpose limitation principle is usefully seen in conjunction with another general principle, that of collection limitation. The principle of collection limitation mandates that only such data should be collected that is necessary for achieving the purposes specified for such processing. Thus, the minimum data necessary for achieving a purpose could be collected, and such data used only for the specified purpose and other compatible purposes and no other. Taken together, these are designed to lead to data minimization that in turn, allows greater granular control for the data principal.[439]

### 4.21.3. Collection Limitation Principle

Collection Limitation Principle is provided in section 6 of this Bill. In section 6, provided following provision related to the collection limitation principles,

*"Collection of personal data shall be limited to such data that is necessary for the purposes of processing"*[440]

It means collection of personal data shall be limited. Data processer firstly decide that the which personal data is required for that specific purpose. Then he collects those personal that is required for processing of personal data. It is the duty of data processer to collect and storage that personal data which is relevant for specific purpose.

### 4.21.4. Lawful Processing Principle

Lawful processing principal is provided in the Section 7 of this bill. It is the duty of the data processer to process lawfully the personal data or sensitive personal data of the data principal. The processing of data is lawfully or not, it is determined by

[438] B.N Krishna Committee Report on "Data Protection in India" 53 (July, 2018).
[439] B.N Krishna Committee Report on "Data Protection in India" 54 (July, 2018).
[440] Section 6 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

the provision of this bill which is given in section 7. According to section 7, there are provide two type provision related to the lawfully data processing,

Firstly, where personal data are processing their regards provision given in the Chapter III of this Bill. Secondly, where sensitive personal data are processing their regards provision given in the Chapter IV of this Bill.

It means whenever the data processer processing our personal data or sensitive personal data then he fulfils the provision of this Bill. If the data processer is not fulfilled the provision of this Bill, then the processing is unlawful.

According to section 7 clause (1) of this bill, whenever data processer is processing of personal data of the data principal then he fallows the provision of Chapter III. In the chapter III provide the provision related to the "Ground for Processing of Personal Data". Chapter III deals the fallowing provision related to the processing of personal data processing, these are,

**(1)** Processing of Personal Data on the basis of consent[441]

**(2)** Processing of Personal Data for function of the state[442]

**(3)** Processing of Personal Data in the compliance with law or any order of any court or tribunal[443]

**(4)** Processing of Personal Data necessary for prompt action[444]

**(5)** Processing of Personal Data necessary for purpose related to employment[445]

**(6)** Processing of Personal Data for reasonable purpose[446]

Same provision is provided in the Chapter IV of this bill for the Processing of Sensitive Personal Data.

[441] Section 12 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[442] Section 13 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[443] Section 14 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[444] Section 15 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[445] Section 16 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[446] Section 17 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

It is the duty of the Data Processer fallow the above mention provision when he processer our personal data. If he not fallows these provisions, then he is the liable for penalties under Section 73 of this Bill.

On the other hand, Chapter V also provide the provision related to the processing of personal data or sensitive personal data of the children. If the processing of personal data or sensitive personal data of the children then the data processer fallow the provision of the section 23 of this Bill.

Processing of data is lawful when data processer is fallow the above mention provision otherwise it is unlawful.

### 4.21.5. Data Quality Principle

The Data Quality Principal is provided in the Section 9 of this Bill. According to section 9 of this Bill,

> "*The data fiduciary shall take reasonable steps to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.*"[447]

Section 11of the Personal Data Protection Act, 2010 also provide the same provision related to the Data Quality (Data Integrity). According to Section 11of the Personal Data Protection Act, 2010,

*"The data user to take reasonable step to ensure that the personal data is accurate, complete, not misleading and kept up-to date by considering the purpose……"*[448]

The principle of data quality implies that the personal data being used should be relevant to the purpose for which it is to be used and should be accurate, complete and kept up-to-date. The requirements of accuracy, completeness and up-to-dateness are also linked to purpose and therefore should meet the requirements of the purpose for which the personal data was collected.[449]

---

[447] Section 9 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[448] Section 11 of "Personal Data Protection Act,2010" (Act of 2010).
[449] B.N Krishna Committee Report on "Data Protection in India" 62 (July, 2018).

Accuracy, completeness and up-to-date of data are the key requirements of data quality. Personal data is intrinsically linked to individuals, who are therefore the most reliable source of data. The primary responsibility to provide accurate data to the data fiduciary will rest on the data principal. However, there is a corresponding obligation to ensure that data is complete, i.e. it will satisfy the purpose for which it was collected on the data fiduciary who is collecting such data.

In instances where personal data has been collected from parties other than the data principal, then the obligation would be on the data fiduciary to ensure accuracy, and in case of data being inaccurate, it is corrected, completed or updated upon request by the data principal. This is in conjunction with the right to correction, etc. which has been provided under our law to all data principals.[450]

Further, there will be a general obligation on the data fiduciary to ensure that the personal data being processed is accurate and to ensure that any onward disclosure or sharing of such data to third parties meets the requirements of accuracy. Where keeping the personal data up-to-date is necessary for the purpose of processing, such as in instances where the purpose relies on data remaining current, the fiduciary will be under a general obligation to take necessary steps to ensure that the data is kept up-to-date over time.[451]

### 4.21.6. Data storage Limitation Principle

Data storage limitation principle is provided in section 10 of this Bill. This principle provided that personal data shall not be retained longa than it is necessary to fulfil the purpose for which it was collected and require the data user to destroy or permanently delete all personal data which is no longer required.[452]

This principle is closely connected to the principle of purpose limitation, envisages that data should be stored by the fiduciary only for a time period that is necessary to fulfil the purpose for which it was collected. Once the purpose has been achieved, the data should be deleted or anonymized. The rationale behind this is that once processing is over, control over the data may be lost, since it is no longer of any

[450] B.N Krishna Committee Report on "Data Protection in India" 62 (July, 2018).
[451] Ibid.
[452] Noriswadi Ismail and Edwin Lee Yong Cieh et.at (eds.) Beyond Data Protection 47 (Springer, London, 2013).

interest to the data fiduciary, which may expose the data to the risk of theft, unauthorized copying or the like.[453]

Data storage limitation principal is provided in Section 10 of this Bill. Section 10 clause (1) provided that,

*"The data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed."*[454]

It means it is the primary duty of the data fiduciary to retain personal data of the data principal. The data fiduciaries will only be able to retain personal data as long as it is required to satisfy the purpose for which it was collected.

In order to avoid any risk of unauthorized access once processing has ceased, the principle of storage limitation will be applicable as an obligation on data fiduciaries. Thus, data fiduciaries will only be able to retain personal data as long as it is required to satisfy the purpose for which it was collected. Thereafter, the said data may be anonymized or erased permanently to meet the requirements of the law. The key requirement is that once the object of processing has been achieved, the data, if retained, should not be capable of identifying any individual.

It is a general rule that data fiduciary to retain personal data of the data principal as long as it is required to satisfy the purpose for which it was collected. But some circumstances given exception of this general rule. These exceptions are provided in section 10 clause (2) of this bill, these are

*"Not withstanding sub-section (1), personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply with any obligation, under a law"*[455]

It means personal data may be retain for a longer period of time if such retention is explicitly mandate under any law or necessary to comply with an obligation under any law. Exception of the principle of storage limitation would be instances where legal or sectoral or regulatory requirements may necessitate the storage of such personal data for further periods.

Section 10 clause (3) provide that

*"The data fiduciary must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession"*[456]

---

[453] B.N Krishna Committee Report on "Data Protection in India" 61 (July, 2018).
[454] Section 10 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[455] Section 10 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

It means it is the duty of data fiduciary to undertake periodic review for the determine that whether it is necessary to retain the personal data in its possession or not. It is burden on data fiduciaries in terms of a periodic review of all personal data retained by them. However, such review is necessary to make fiduciaries conscious of the personal data in their possession so that they can act, in a timely manner, to avoid any future breaches.

Further, as long as the personal data is retained by the data fiduciary, it will be liable for all obligations that are imposed on it by the data protection law. The obligations will continue till the data has either been erased permanently or has been anonymized by the fiduciary. Therefore, obligations would continue to apply even after processing has ceased, as the data retained by the fiduciary remains capable of identifying individuals thereby qualifying as personal data.

### 4.21.7. Notice and Choice Principal (Transparency Principal)

In securing the rights of the data principal under data protection law, a prime barrier faced by data principals is the lack of information on how their personal data comes to be processed. Especially in the digital context, it becomes difficult for a data principal to know and understand whether, by whom and for what purpose personal data about her is being collected and processed. In this regard, it is essential that processing be carried out transparently. It means all information related to the data processing communicate the data principal. This not only bolsters the fairness of the processing activities, ensuring that data principals can trust them, but also makes sure that data fiduciaries are accountable by creating some scope for principals to challenge them.[457]

In this regard Section 8 provide provision related to the notice principle. According to section 8(1) of this Bill, it is the duty of data fiduciary to communicate the all information to the data principal which is related to the data processing. It is necessary that the communication of these information is not latter than at the time of collection of personal data. Section 8 clause (1) provide fallowing provision related to the data processing,

[456] Section 10 Clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[457] B.N Krishna Committee Report on "Data Protection in India" 58 (July, 2018).

*"The data fiduciary shall provide the data principal with the following information, no later than at the time of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable—*

*(a) the purposes for which the personal data is to be processed*

*(b) the categories of personal data being collected;*

*c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable……."*[458]

It means a data fiduciary is obliged to provide notice to the data principal no later than at the time of the collection of her personal data. If the data is not being collected from the principal directly, this obligation is still applicable, and the fiduciary must provide the notice as soon as is reasonably practicable. The information that a fiduciary is required to disclose to the data principal has been specified to ensure that it alleviates, as best as is possible, the problems of opacity, uncertainty, lack of clarity, and lack of accountability because of which privacy harms are caused. Not only must the data principal be informed as to who is processing what personal data of theirs for what purposes, they must also be told various points of relevant information including the basis of processing, their ability to withdraw consent (if processing is based on consent), any legal obligations on the basis of which the processing is taking place, information regarding any cross-border transfer of the personal data that that the data fiduciary intended to carry out, the period for which the personal data will be retain, persons with whom the data may be shared, the period of retention of data, as well as the procedure for the exercise of data principal rights, the procedure for grievance redressal and the right to file complaints with the Data Protection Authority.[459]

These points of information must be conveyed to the Data principal in all circumstances except where processing is taking place for emergency situations requiring prompt action.

Section 8 clause (2) provided the fallowing provision, these are

*"The data fiduciary shall provide the information as required under this section to the data principal in a clear and concise manner that is easily*

[458] Section 8 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[459] B.N Krishna Committee Report on "Data Protection in India" 58 (July, 2018).

*comprehensible to a reasonable person and in multiple languages where necessary and practicable."*[460]

It means it is the duty of data fiduciary to provide information as required under this section to the data principal in clear and concise manner. It must also be ensured that the form of the communication is clear and concise so that it is easily comprehensible. There may also be various situations where it is necessary for the information to be communicated in multiple languages.

### 4.22. Processing of Personal Data and Sensitive Personal Data

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. Section 12 of this bill dealt the provision related to the Processing of personal data on the basis of consent. Here consent means, consent of the data principal. That consent given before the commencement of the data processing. It is necessary that, the consent should be valid.

Section 12 of this bill provide that the consent principal. according to this principal when any person processing our personal data, then it is required that the processing our personal data on the basis of consent of the data principal. It is necessary that the consent should be valid. According section 12 clause (2), consent deemed valid when it fulfils the fallowing conditions, that is,

Consent shall be,

(1) Free
(2) Informed
(3) Specific
(4) Clear
(5) Capable of being withdrawn

Here free consent means, consent given accordance with the section 14 of the Indian Contract Act 1872. It means consent of data principal not taken in coercion,

[460] Section 8 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

undue influence, fraud, misrepresentation, mistake. If it's taken by coercion, undue influence, fraud, etc. then consent is not valid.

The word "Informed" having regards to whether the data principal has been providing with the information required under section 8 of this bill. Consent specific means, consent of data principal is specific in respect of purpose of processing. Word "Clear" having regards that, consent is indicated through an affirmative action that is meaningful in a given context.

Notwithstanding the above mention consent principal, the data subject's consent is not required to be obtained if the processing is necessary for;

(1) Function of the State
(2) In compliance with law or any order of any court or tribunal
(3) For prompt action
(4) For purpose related to employment

Section 13 of this bill provide provision related to the processing of personal data for the function of the state. According to this section, consent of the data principal is not necessary where personal data processed for

**(a)** any function of Parliament or State legislature
**(b)**For the exercise of any action function of the state authority by law
  (i) For any service or benefit to the data principal for the state, or
  (ii) Issuance of any certification, license, or permit of any action or activity of the data principal by the state[461]

Same provision provided in section 19 of this bill for the processing for Sensitive personal data.

Provision related to the Processing of personal data in compliance with law or any order of any court is provided in section 14 of this bill. Word "compliance with law" means provision of data processing explicitly mandate under any law made by parliament or any state legislature. Same provision provided in section 20 of this Bill for the processing of sensitive personal data in compliance with law or any order of any court or tribunal.

[461] Section 13 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

Section 15 of this bill provide provision related to the processing of personal data necessary for prompt action. Where prompt action necessary, their consent principal is not applied for data processing. Word "prompt action" include

(a) Any medical emergency involving a threat to the life or threat to the health of data principal or any individual
(b) Medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health.
(c) During any disaster or any breakdown of public order[462]

same provision provided in section 21 of this for the processing of Sensitive personal data necessary for prompt action.

Section 16 of this Bill provide provision related to the "Processing of Personal Data Necessary for purpose related to employment". According to section 16 clause (1) of this bill, where data principal is employee of the data fiduciary, Personal data may be processed if such processing is necessary for the

(a) Recruitment or termination of employment of a data principal
(b) Provision of any service or benefit sought by the data principal
(c) Verify the attendance of the data principal
(d) Any other activity relating to the assessment of the performance of the data principal[463]

Section 17 of this bill provide provision related to the processing of data for reasonable purpose. It is additional ground for processing of personal data, which is other than ground provided in section 12 to section 16. The word "Reasonable purpose" is include the fallowing activity,

(a) Whistle blowing

(b) Prevention and detection of any unlawful activity including fraud

(c) Network and information security

(d) Mergers and acquisitions

[462] Section 15 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[463] Section 16 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

(e) Recovery of debt

(f) Credit scoring

(g) Processing of publicly available personal data[464]

Data protection authority have power to specifies the reasonable ground for data processing. Where the authority specified the reasonable purpose, it is the duty of the authority to

(a) Lay down such safeguard which is appropriate to ensure the protection of the right of data principal,
(b) Determine where the provision of notice under section 8 would not apply having regards to whether such provision would substantially prejudice the relevant reasonable purpose.[465]

Chapter V dealt the provision related to the processing of personal data and sensitive personal data of children. It is the duty of data fiduciary to protect the right and interest of the child data principal. It is the duty of data fiduciary to verifies the age of children. In this regards data fiduciary incorporated appropriate mechanism for age verification and parental consent.

According to section 23 clause (1) of this bill,

*"Every data fiduciary shall process personal data of children in a manner that protects and advances the rights and best interests of the child."*[466]

It means, it is the mandatory duty of the data fiduciary to process personal data of a child in prescribed manner. That manner protects and advance the rights and best interests of the child. In this regard data fiduciary incorporate appropriate mechanisms for age verification and parental consent. Where the appropriate mechanisms are incorporated by data fiduciary shall be determined on the basis of

(a) Volume and proportion of such personal data
(b) Possibility of harm to children arising out of processing of personal data[467]

[464] Section 17 clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[465] Section 17 clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[466] Section 23 clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

Generally parents or relative of the child is the guardian of the child in the matter of data processing, but some time Data Protection Authority have power to decide the guardian of the children in the matter of data processing. Authority notify the fallowing as guardian,

(a) Data fiduciary who operate commercial website or online services directed at children
(b) Data fiduciaries who process large volume of personal data of children[468]

Guardian data fiduciary have right to taken necessary action for the processing of personal data or sensitive personal data of children. This right of data fiduciary is not absolute, it is restricted by section 5 clause (5) of this bill. According to this section guardian data fiduciary shall be barred from,

(a) Profiling
(b) Tracking
(c) Behavioral monitoring
(d) Targeted advertising directed[469]

Which can cause significant harm to the child.

### 4.23. Rights of Data Principal

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. Specifically, some of these rights can be said to flow from the freedom of speech and expression and the right to receive information under Article 19(1)(a) and Article 21 of the Constitution. A strong set of data principal rights is an essential component of an empowering data protection law.

---

[467] Section 23 clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[468] Section 23 clause (4) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[469] Section 23 clause (5) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

This 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

These rights are the essential component of the empowering data protection law.

### 4.23.1. Right to Confirmation and Access[470]

The right to confirmation refers to the right of a data principal to inquire regarding processing of his personal data by a data fiduciary. The right to access refers to the right of the data principal to gain access to her personal data which is stored with the data fiduciary. This right enables a data principal to gain access to a copy of all the personal data held about him by an entity. The basis of these rights is to ensure that the data principal can understand, gauge and verify the lawfulness of processing.[471]

The rights to confirmation and access enable a data principal to enforce the substantive obligations of data fiduciaries. Only when a data principal knows what personal data a fiduciary has about himself and how it has been used, can he enforce his rights against the fiduciary. It is important to note that without the right to confirmation and access, the substantive obligations may become mere platitudes. Thus, in principle the rights to confirmation and access must find place in the law.[472]

Section 24 of this Bill provided that "right to confirmation and access".

According to this section, data principal has right to obtain,

(a) Confirmation about the personal data of the data principal, which is processing or processed by the data fiduciary
(b) Brief summary of the personal data, which is processing or processed by the data fiduciary

[470] Section 24 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[471] B.N Krishna Committee Report on "Data Protection in India" 69 (July, 2018).
[472] Ibid.

(c) Brief summary of processing activities under taken by the data fiduciary , its also include any information provided in the notice under section 8 in relation to such processing activities[473]

According to section 24 clause (2) of this bill, where data fiduciary is provided such information, brief summary of the personal data of data principal, there is the duty of the data fiduciary to give such information in a clear and concise manner which is easily comprehensible to a reasonable person.

The scope of these rights must be guided by their rationale. These rights allow the data principal to take action, in case there is a breach of a substantive obligation by the fiduciary and are tools which a data principal can use to gauge the lawfulness of data handling by the data fiduciary. Keeping this in mind, the scope of the right to access and confirmation should be broad, and must include,

**(i)** All personal data relating to the data principal that has been collected by the data fiduciary

**(ii)** The purposes for which the data fiduciary has collected such data;

**(iii)** The entities or persons to whom such data has been disclosed;

**(iv)** Information regarding cross-border transfer of such data;

**(v)** Information regarding the estimated duration for which data is stored, if feasible

**(vi)** Such other information regarding the collection, storage, handling and sharing of personal data that would have been provided under the obligation of notice that may need to be accessed again for transparent disclosure to the data principal.[474]

Data fiduciaries cannot refuse access to data principals on the basis of grounds such as disproportionate effort, costs, volume of data, technical feasibility, inadequate manpower, frivolous claims or any other alternate remedy. The only grounds for such refusal can be any relevant exemptions contained in this law, or any other law, or any other general conditions of refusal for any data principal right.

[473] Ibid.
[474] B.N Krishna Committee Report on "Data Protection in India" 70 (July, 2018).

### 4.23.2. Right to correction[475]

Section 25 of this bill provide the provision related to the right to correction of data principal.

A data principal shall have the right to correct, complete or update any inaccurate or incomplete personal data about her. It empowers data principals to ensure accuracy of their personal data and may be a natural consequence of the right to access personal data, where such personal data is accessed and found to be inaccurate. The application of this right has a broad scope covering information about the data principal that a fiduciary possesses. It applies to both input personal data and output personal data. Input personal data refers to the data that the data principal provides to the data fiduciary whereas output personal data refers to the data that has been used to create a profile or reach a certain conclusion about an individual.

It is important to maintain correct and up-to-date personal data in order to ensure the veracity of output decisions. This right is a necessary corollary to implementing the obligation to maintain accurate personal data, which is an obligation on data principals and data fiduciaries.

In this regard, data fiduciaries cannot charge any fee for the implementation of the right to correction as it is the responsibility of the data fiduciary to ensure accuracy of personal data, when it holds such data.

### 4.23.3. Right to Data Portability[476]

Data portability refers to the ability to move, copy or transfer data easily from one database, storage or IT environment to another. Data portability primarily enables individual end user or enterprises to seamlessly move, interested and interlink datasets within disparate system. Data portability concerns are especially common in cloud compounding solutions when data needs to be transferred from an in-house facility or from the cloud to another location in the cloud.[477]

---

[475] Section 25 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[476] Section 26 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[477] https://www.techopedia.com/definition/6725/data-portability (visited on September 21,2018).

Right to data portability of data principal is provided in section 26 of this bill. Section 26 clause (1) provided that,

*"The data principal shall have the right to—*

*(a) Receive the following personal data related to the data principal in a structured, commonly used and machine-readable format—*

*(i) which such data principal has provided to the data fiduciary;*

*(ii) which has been generated in the course of provision of services or use of goods by the data fiduciary or*

*(iii) which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained."*[478]

Above mention provision only apply where the processing is carried out through automated means. It does not apply where the processing has been carried out through the

(a) Processing is necessary for the function of the state under section 13
(b) Processing is compliance of law as referred to in section 14
(c) A trade secret of any data fiduciary[479]

The right to data portability is critical in making the digital economy seamless. This right allows data principals to obtain and transfer their personal data stored with a data fiduciary for the data principal's own uses, in a structured, commonly used and machine-readable format. Thereby, it empowers data principals by giving them greater control over their personal data. Further, the free flow of data is facilitated easing transfer from one data fiduciary to another. This in turn improves competition between fiduciaries who are engaged in the same industry and therefore, has potential to increase consumer welfare. As the right extends to receiving personal data generated in the course of provision of services or the use of goods as well as profiles created on the data principal, it is possible that access to such information could reveal trade secrets of the data fiduciary. To the extent that it is possible to provide

[478] Section 26 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[479] Section 26 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

such data or profiles without revealing the relevant secrets, the right must still be guaranteed. However, if it is impossible to provide certain information without revealing the secrets, the request may be denied. The right to transfer or transmit data from one fiduciary to the other should however be limited by constraints of technical feasibility. That is, data fiduciaries would not be obligated to provide data portability if they are able to prove that technical capabilities as currently existing would make the required access or transfer unfeasible.[480]

### 4.23.4. Right to Be Forgotten

The right to be forgotten or "the right to be erased" allow an individual to request for removal of his personal information /data online. The origin of this right can be traced back to the French jurisprudence on the 'right to oblion'.[481]

The right to be forgotten in the digital sphere refers to the right of individuals to request data controllers to erase any data about them from their systems. The principal driver behind the idea of the right to be forgotten is the massive expansion in the availability and accessibility of information associated with the digital world of the Internet.[482]

The right to be forgotten is an idea that attempts to instill the limitations of memory into an otherwise limitless digital sphere. A limited memory and the consequent need to both remember and forget are essential facets of the human condition. The internet, with its currently vast reserves of data storage appears to facilitate timeless memory. As a result, the ability to forget is seriously denuded. This might not be entirely undesirable— collective attempts at forgetting have often involved attempts at rewriting history.

However, the individual desire to forget is an expression of autonomy that may be worthy of protection. This is especially the case, if we accept that data flows are initiated by the individual who must be free and to whom others must be fair. But in considering such a right, it is imperative to note that other individual freedoms and collective goods may be impacted. Removing publicly available information takes

[480] B.N Krishna Committee Report on "Data Protection in India" 75 (July, 2018).
[481] https://www.livelaw.in/first-indian-court-up-hold-rights (visited on September 22,2018).
[482] B.N Krishna Committee Report on "Data Protection in India" 62 (July, 2018).

away from an individual's right to know; at the same time, it abridges the freedom of the press which has published the story in the first place. Further, if every individual started exercising a right to be forgotten over various types of personal data, the nature of the public realm of information itself would be brought into question as such information may be permanently deleted. Of particular concern is the risk that the deletion may be not just from the public space but also from private storage, preventing later publication as well. Therefore, in order to address these free speech concerns, there may be a need to make a distinction between restrictions on disclosure (such as delinking in search results) and permanent erasure from storage, which may not be permitted as a separate individual participation right. Further, any implementation of this limited right to be forgotten must involve a careful consideration of the following principled and practical issues:

The Indian judiciary through the Karnataka High Court in Sri Vasunathan v. The Registrar General[483] has recognized the right to be forgotten and safeguarded the same in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned, in particular. Further, the importance of a right to be forgotten was further emphasized by the Supreme Court in Puttaswamy. The Supreme Court opined that,

"*the impact of the digital age results in information on the Internet being permanent. Moreover, any endeavor to remove information from the Internet may not result in its absolute obliteration. It is thus, said that in the digital world preservation is the norm and forgetting a struggle.639 People are not static; they are entitled to re-invent themselves and correct their past actions. It is privacy which nurtures this ability and removes the shackles of unadvisable things which may have been done in the past."*

Therefore, the recognition of the right to privacy envisages within its contours the right to protect personal information on the Internet. Consequently, from this right, it follows, that any individual may have the derivative right to remove the 'shackles of unadvisable past things' on the Internet and correct past actions.

[483] 2017 SCC Kar 424.

In section 70 of this bill, provide penalty for failure to comply with data principal request under this chapter. According to this section , if data fiduciary is failure to comply with any request made by a data principal, without any reasonable explanation , such data fiduciary is shall be libel to a penalty of five thousand rupees for each day during which such default continue.[484]

### 4.24. Duty and Obligations of Data Fiduciary

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.

#### 4.24.1. Duty to Maintain Data Privacy

Data privacy is the core issue of this bill. So, it is the duty of data fiduciary to maintain the data privacy. In this regard, section 29 provide provision related to privacy. According to section 29 of this bill, it is the duty of data fiduciary to implement the policies which is related to the data privacy. it is also the duty of data fiduciary to ensure that,

(a) Managerial, Organisational, business practice and technical system are designed in a manner to anticipated, identify and avoid harm to the data principal

[484] Section 70 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

(b) The obligation mentioned in chapter II are embedded in Organisational and business practice

(c) Technology used in the processing of personal data is in accordance with commercially accepted

(d) Privacy is protected throughout processing from the point of collection to deletion of personal data

(e) Processing of personal data is carried out in a transparent manner

(f) The interest of the data principal is accounted for at every stage of processing of personal data[485]

For, maintain data privacy data fiduciary implement data privacy policies which is draft by appropriate authority. It is the duty of data fiduciary to ensure that, all data protection principal is fallowed by the appropriate authority to processing our personal data.

### 4.24.2. Duty to Maintain Transparency

Section 30 of this bill provide provision related to the transparency. According section 30 clause (1) of this bill, it is the duty of data fiduciary to maintain transparency. In this regard, it is the duty of data fiduciary to take reasonable steps to maintain transparency. This regard adapts the general practice related to processing of personal data. It is the duty of data fiduciary to make the fallowing information available and easily accessible form, as may be specified-

**(a)** Category of personal data generally collected and manner of such collection

**(b)** Purpose for which personal data is generally processed

**(c)** Categories of personal data processed in exceptional situation or any exceptional purpose of processing that create a risk of significant harm

**(d)** Existence of aright to file complaint to the authority

**(e)** Information regarding cross- border transfer of personal data[486]

According to section 30 clause (2) of this bill,

It is the duty of data fiduciary to periodically notify the data principal, to important operations in the processing of personal data.[487]

[485] Section 29 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[486] Section 30 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

### 4.24.3. Duty to Maintain Security Safeguards

Section 31 of this bill provide provision related to security safeguard of personal data. According to section 31 clause (1) of this bill, it is the duty of data fiduciary and data processer to implement appropriate security safeguard for the prevent from harm, that may be result from personal data processing. In this regard, which security safeguard is adapted, it's depend on the nature, scope, and purpose of processing of personal data of the data principal.

According this section, appropriate security safeguard also includes the,

(a) Use of methods such as de-identification and encryption
(b) Steps necessary to protect the integrity of personal data
(c) Steps necessary to prevent misuse, unauthorized access, modification disclosure or destruction of personal data.[488]

According to section 31 clause (2) of this bill,

It is the duty of data fiduciary and data processer, to periodically review the security safeguards which is provide in section 31 of this bill, for the data security.

### 4.24.4. Duty to Notification for Breach of Personal Data

With large amounts of data being held by fiduciaries, the breach of personal data becomes a real possibility. A breach can have deleterious consequences for individuals whose personal data has been subject of the breach. Therefore, it becomes important to inform data principals about such instances so that they can take suitable measures to shield themselves from their harmful consequences. However, due to considerations of adverse publicity and avoidance of liability, fiduciaries may be dis-incentivized from reporting incidents of breach to individuals. Thus, a notification to the Data Protection Authority (DPA) upon the occurrence of a breach has been envisaged, in keeping with trends in other jurisdictions, before a notification to the individual is made. It may be noted that such personal data breaches that are subject to

[487] Section 30 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[488] Section 31 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

obligations of notification should not be confused with breaches of data protection law generally. [489]

The definition of personal data breach[490] will be structured in a manner that accounts for the three key principles of information security i.e. confidentiality, integrity and availability. These principles offer the most holistic understanding of breach and comprehensively cover all the possible facets of a breach. Confidentiality breach implies an unauthorized or accidental disclosure of, or access to, personal data. Integrity breach constitutes an unauthorized or accidental alteration of personal data. An availability breach occurs when there is an accidental or unauthorized loss of access to, or destruction of, personal data. A particular breach may however not fit neatly into any of these categories but may be combination of these. The significant elements of the definition of personal data breach would be the occurrence of 'disclosure' or 'access', 'alteration', and 'loss of access' or 'destruction' of personal data which occurs in manner that is either 'accidental' or 'unauthorized'.[491]

Section 32 of this bill provide provision related to personal data breach. According to section 32 clause (1) of this bill, it is the duty of data fiduciary to notify the data protection authority when the personal data breach and such breach is likely to cause harm to any data principal. It is the duty of data fiduciary to give notification to data protection authority, related to breach of personal data. The word "Notification" include the fallowing particulars also,

**(a)** Nature of personal data which is subject matter of the breach
**(b)** Number of data principals affected by the breach
**(c)** Possible consequences of the breach
**(d)** Measure being taken by the data fiduciary to remedy the breach[492]

Notification is made by data fiduciary to the authority as soon as possible which is not latter than the time period specified by the authority.

The content of such notification should at the minimum include the nature of personal data that has been subject to breach and the number of individuals who have

[489] B.N Krishna Committee Report on "Data Protection in India" 63 (July, 2018).
[490] Section 3 Clause (30) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[491] B.N Krishna Committee Report on "Data Protection in India" 64 (July, 2018).
[492] Section 32 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

been affected by the breach, the possible consequences of the breach and the measures being taken to contain the breach.

After becoming aware of such a breach, the fiduciary will be required to comply with the notification requirement as soon as possible. The obligation is being envisaged as a layered one where the fiduciary will be required to be in continuous communication with the data protection authority regarding the measures being taken to identify the scope and extent of the breach and the procedures being adopted to contain the breach. Though the obligation is to notify the Data Protection Authority as soon as the circumstances surrounding the breach permit the fiduciary to do so, an outer limit for such notification should nonetheless be set so as to prevent risk of misuse.[493]

According to section 32 clause (5) of this bill,

Upon notification, the DPA shall have the power to decide the severity of the breach and if relevant, the manner in which it needs to be reported to the individuals whose data has been breached. The breach should be notified to the individuals in instances where such a breach not only poses harm to the data principals, but also where some action is required on part of the principals to protect themselves from the consequences of the breach. The DPA has been granted the powers to determine when and how such notification is required to prevent the fiduciary from making a unilateral decision in this regard which may be motivated by factors other than best interests of the data principals.[494]

According to section 32 clause (6) of this bill,

The DPA is expected to better guide the actions of the data fiduciary and suggest or direct remedial measures, and it must be ensured that liability for the breach is suitably accorded in an adjudication action. Failure to notify a breach would make the fiduciary liable to penalty under the provisions of this bill.[495]

[493] B.N Krishna Committee Report on "Data Protection in India" 64 (July, 2018).
[494] B.N Krishna Committee Report on "Data Protection in India"64 (July, 2018).
[495] Ibid.

### 4.24.5. Maintain Personal Data Record

Section 34 of this bill provide provision related to maintain data record. According to this section, it is the duty of data fiduciary to maintain accurate and up-to-date records. To maintain accurate and up-to-date records, which is mention fallowing-

(a) Important operations in the data life-cycle including collection, transfer, and erasure of personal data to demonstrate compliance as required under section 11
(b) Periodic review of security safeguards under section 31
(c) Data Protection Impact assessment under section 33
(d) Any other aspect of processing as may be specified by the authority[496]

Maintain of such records as specific form which is specified by the authority.

### 4.24.6. Appointment of data protection officer

Section 36 of this bill provide provision related to the appointment of data officer. It is the duty of data fiduciary to appoint data protection officer for the providing information and advice to the data fiduciary on matter relating to fulfilling its obligation under this act. Data officer shall be appointed for the fallowing functions, that is

(a) Monitoring personal data processing activities of the data fiduciary to ensure that such processing dose not violet the provision of this Act
(b) Providing information and advice to the data fiduciary on matter relating to fulfilling its obligation under this Act
(c) Providing assistance to and co-operation with the authority on matter of data compliance of data fiduciary with provision under this Act
(d) Maintaining an inventory of all records maintained by the data fiduciary pursuant to section 34[497]

Data protection officer is appointed by the data fiduciary for carrying out the above mention function.

[496] Section 34 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[497] Section 36 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

### 4.24.7. Duty to Provide Grievance

**Section** 39 of this bill provide provision related to Grievance Redressal of data principal. According to section 39 clause (1) of this bill, it is the duty of data fiduciary to place proper procedure and effective mechanism to address grievance of data principal efficiently and speedy manner[498].

According to section 39 clause (2) of this bill, when violation of any provision of this Act, prescribed rule regulations thereunder, and due to this violation causes harm or likely to causes harm to data principal, then it is the right of the data principal to rise grievances to-

(a) Data protection officer, in case of a significant data fiduciary
(b) An officer designated for this purpose, in case of any other data fiduciary.[499]

It is the duty of data fiduciary to resolved the grievances in an expeditious manner and no longer than thirty days from the date of receipt of grievances by data fiduciary.[500] Where grievances are not resolved within the specified period or resolved but data principal is not satisfied with the manner in which the grievances is resolved or data fiduciary has reject the grievances, then the data principal have right to file a complaint with the adjudication wing under section 68 of this bill in prescribe manner.[501]

Any person who aggrieved by any order made under this section, have right to appeal to the Appellate Tribunal.[502]

## 4.25. Transfer of Personal Data Outside India

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

[498] Section 39 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[499] Section 39 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[500] Section 39 Clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[501] Section 39 Clause (4) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[502] Section 39 Clause (5) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

the physical economy in India where a combination of free movement of goods and transfer restrictions operate alongside each other. The key questions are where and how the line can be drawn in determining which data can be transferred across borders.

Section 40 of this bill provide provision related to "Restriction on Cross-Border Transfer of Personal Data". According to section 40 clause (1) of this bill, it is the duty of data fiduciary to ensure that at least one serving copy of personal data storage on a server or data center located in India.[503] It is the duty of Central Government to notify categories personal data as critical personal data that shall only be processed in a sever or data center located in India.[504] When the central government notify the category of critical personal data, then it is the duty of central government to exempt the State on the ground of necessity or strategic interest, from the requirement of the section 40 subsection (1) of this bill.[505] But this provision is not apply to Sensitive personal data.[506]

Section 41 provide provision related to "Cross-Border transfer of personal data". According to sub-section (1) of section 41, personal data may be transferred outside the territory of India. In this section, personal data means "other than those categories of sensitive personal data which is under sub-section (2) of section 40 of this bill. Personal data may be transfer outside the territory of India where-

(a) Transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the authority
(b) Central government, after consultation with the authority, has prescribed that transfer to a particular country, or to a sector within a country or to a particular International Organization is permissible
(c) Authority approves a particular transfer or set of transfer as permissible due to situation of necessity[507]

Sub-section (3) of section 41, provide provision related to the transfer of sensitive personal data, which is notify by the central government, outside India.

[503] Section 40 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[504] Section 40 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[505] Section 40 Clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[506] Section 40 Clause (4) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[507] Section 41 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

According to this section these types of sensitive personal data may be transfer outside the territory of India –

(a) To a particular person or entity engaged in the provision of health service or emergency service where such transfer is strictly necessary for prompt action under section 16
(b) To a particular country, or a prescribe sector within a country or to a particular International Organization that has been prescribed under clause (b)of sub-section (1) of section 41.[508]

Where such type of data transfer, shall be notified to the authority within such time period as may be prescribe.[509]

**4.26. EXEMPTION**

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

[508] Section 41 Clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[509] Section 41 Clause (4) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

### 4.26.1. Security of the state[510]

National security is a nebulous term, used in statutes of several jurisdictions to denote intelligence gathering activities that systematically access and use large volumes of personal data. The ostensible purpose of such processing is to continuously gather intelligence to prevent attacks against the country, whether internal or external. Though always an incident of state power, the pervasiveness of such intelligence gathering has significantly expanded in the data economy. It is thus critical to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception.[511]

According to section 42 of this bill, where the processing of personal data in the interest of the security of the state shall not be permitted unless it is authorized pursuant to a law and accordance with the procedure stablished by such law.

### 4.26.2. Prevention, detection, investigation and prosecution of contraventions of law[512]

Prevention, detection, investigation and prosecution of contraventions of law are important state functions, central to the protection of individuals and the society at large. It is a legitimate aim of the state. The state enjoys a monopoly of the legitimate use of physical force to enforce order within its sovereign territory. The Constitution entrusts State Governments and Union Territories with the maintenance of law and order, including ―prevention, detection, registration, investigation and prosecution of crimes. While these activities are in pursuance of a legitimate aim of the state, they must meet the "Test of necessity and proportionality", as laid down in Puttaswamy case.[513]

According to section 43 of this bill, where the processing of personal data in the interest of the prevention, detection, investigation, etc. shall not be permitted unless it is authorized by law made by parliament or State legislature.

[510] Section 42 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[511] B.N Krishna Committee Report on "Data Protection in India" 122 (July, 2018).
[512] Section 43 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[513] B.N Krishna Committee Report on "Data Protection in India" 129 (July, 2018).

### 4.26.3. Processing for the purpose of legal proceeding[514]

Non-disclosure provisions in the data protection law will be inapplicable to disclosure of personal data necessary for enforcing any legal right or claim, for seeking any relief, defending any charge, opposing any claim, or obtaining legal advice from an advocate in an impending legal proceeding.[515]

Under the Indian data protection law, disclosure of personal data and sensitive personal data in pursuance of a legal claim would occur if it is required to be produced in connection with any legal proceeding (including in preparation for a legal proceeding to be initiated in the future), or where required to establish, exercise or defend legal rights; or where it is required to be brought to the attention of an advocate for seeking legal advice for an impending legal proceeding. Additionally, processing of personal data by any court or tribunal necessary for the exercise of judicial function shall be exempted.[516]

### 4.26.4. Research, archiving or statistical purposes[517]

The Constitution recognizes the development of scientific temper, humanism and the spirit of inquiry and reform as one of the fundamental duties of every Indian citizen. In the context of data protection, the need for this exemption arises because certain principles of data protection such as consent, purpose specification, storage limitation and certain data principal rights may not apply, may be at odds with the achievement of research purpose or may prove to be too onerous to fulfil. The intention behind such exemption is to encourage scientific temper and ensure that larger societal interests, such as innovation and spread of knowledge continue without being unduly restricted.[518]

The research exemption is not being envisaged as a blanket exemption. Only those obligations should be exempted where it is necessary to achieve the object of the research in public interest. Cases in which obligations may have to be exempted are however contextual and dependent on the nature of the research.

---

[514] Section 44 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[515] B.N Krishna Committee Report on "Data Protection in India" 135 (July, 2018).
[516] B.N Krishna Committee Report on "Data Protection in India" 130 (July, 2018).
[517] Section 45 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[518] B.N Krishna Committee Report on "Data Protection in India" 136 (July, 2018).

### 4.26.5. Personal or domestic purposes[519]

According to Section 46 of this bill, where personal data processed by a natural person in the course of purely personal or domestic purpose, shall be exempted by the provision of this bill.

### 4.26.6. Journalistic purposes[520]

A good data protection law needs to achieve a balance between competing social interests. One such conflict exists between the right to free flow of information through freedom of speech and expression and the right to restrict such flow in the interest of privacy and safeguarding of the handling of personal data.

Citizens have the right to protect their privacy and the publication of personal information. To be able to give effect to both these rights, it is essential to ensure a balance between the freedom of expression and the safeguarding of personal data for the public good of a free and fair digital economy. This can be done by allowing recourse to the journalistic exemption where public interest in the disclosure of the personal data is overriding.[521]

According to section 47 of this bill, where the processing of personal data is necessary for or relevant to a journalistic purpose, provision of this bill shall not apply.

### 4.26.7. Manual processing by small entities[522]

The obligations placed on data fiduciaries as a part of data protection law are largely aimed at ensuring that data principals are not subjected to privacy harms and the obligations placed on fiduciaries are thus designed to mitigate and prevent the harms caused by risky practices arising out of electronic data processing using automated means. Such technologies substantially increase the risk of harm from

[519] Section 46 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[520] Section 47 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[521] B.N Krishna Committee Report on "Data Protection in India" 140 (July, 2018).
[522] Section 48 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

personal data processing due to the added ease of recording, dissemination, viewing and systematic analysis[523].

According to section 48 of this bill, where the personal data is being processing manually by a small entity, some provision of this bill shall not apply, these provisions are-

(a) Section 8, 9 10
(b) Clause (c) of sub-section (1) of section 24, and section 26, 27
(c) Section 29 to section 36, and section 38 and 39[524]

It means, it is necessary to ensure that entities carrying out manual processing are subject to data protection law, it is also important to ensure that any exemption from burdensome obligations that has been designed specifically for them does not become a loophole through which organizations execute their most harmful activities.

### 4.27. Data Protection Authority of India

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

### 4.27.1. Establishment and incorporation of authority[525]

According to 49 of this bills, Central Government have power to establish a Data Protection Authority for the purpose of this bill[526]. Data Protection Authority of

[523] B.N Krishna Committee Report on "Data Protection in India" 147 (July, 2018).
[524] Section 48 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[525] Section 49 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[526] Section 49 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

India shall be a legal personality. It's had the right to sue and other person have right to be sued against the Authority.[527]

### 4.27.2. Composition and qualification for appointment of members[528], Removal of members[529]

According to section 50 of this bill, authority shall have consisted,

I. A chairperson
II. Six whole-time members

The chairperson and the members of the authority appoint by the central Government on the recommendation of selection committee. The chairperson and members of the Authority shall be person of ability integrity and standing. They have specialized knowledge in this field. They have required also ten years professional experience in the field of data protection, information technology, cyber and internet law etc.

According to section 52 of this bill, Central Government have power to remove the chairperson or members from his office on the fallowing grounds,

(a) Adjudged an insolvent
(b) Become physically or mentally incapable of acting as a chairperson or members
(c) Convicted of an offence, which involves moral turpitude

On the above mention grounds, the central Government have power to remove the chairperson and members from his office.

### 4.27.3. Power and Functions of the authority[530]

According to section 60 of this bill, it is the duty of the authority to protect the interest of data principals, prevent misuse of personal data, ensure compliance with the provision of this Act and promote awareness of data protection.[531]

[527] Section 49 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[528] Section 50 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[529] Section 51 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[530] Section 60 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

For the above mention obligations authority have the fallowing function, that is

(I) Monitoring and enforcing application of the provision of this Act

(II) specifying residuary categories of sensitive personal data under section 22 of this Act

(III) taking prompt and appropriate action in response to a data security breach in accordance with the provisions of this Act

(IV) monitoring cross-border transfer of personal data undersection 41 of this Act;

(V) promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data

(VI) promoting awareness among data fiduciaries of their obligations and duties under this Act

(VII) monitoring technological developments and commercial practices that may affect protection of personal data

(VIII) promoting measures and undertaking research for innovation in the field of protection of personal data

(IX) specifying fees and other charges for carrying out the purposes of this Act

(X) receiving and handling complaints under the provisions of this Act;

(XI) calling for information from, conducting inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of this Act

### 4.27.4. Power of authority to issue direction[532]

According to section 62 of this bill, authority have power to issue direction time to time for the discharge of his function under this bill. Data fiduciary or data processer generally or partially bound by such direction. When the authority issue such direction then he gives a reasonable opportunity of being heard to the data fiduciary or data processer concerned.

[531] Section 60 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[532] Section 62 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

### 4.27.5. Power of authority to call for information[533]

According to section 63 of this bill, authority have power to call for information to the data fiduciary or data processer, which is reasonably acquired by them in the function of this Act. Where the authority required the information from the data fiduciary or data processer, there are the duty of authority to provide a written notice to the data fiduciary or data processer to stating the reason for such requisition.

## 4.28. Penalties and Remedies

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

Under section 69 of the Bill, two type of penalty are prescribed-

I. Up to Rs. 5 crores or 2 percent of the total worldwide turnover of the preceding financial year[534]
II. Up to Rs. 15 crores or 4 percent of the worldwide turnover of the preceding financial year[535]

These are prescribed for violation of the data protection law and these are awarded by the Adjudicating Officer or Adjudicating wings of the data protection Authority.

Where a data fiduciary who fails to adhere to the data protection principles, such as requirement for notice, take inadequate consent, or does not provide the data principal with the option of withdrawing his consent, will be punishable with higher level of penalty.[536]

Where the processing is without a lawful basis processing, such as consent for a private company or in accordance with a law of the state will also be liable with the higher level of punishment.[537]

---

[533] Section 63 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[534] Section 69 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[535] Section 69 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[536] Section 69 Clause (2) (b) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[537] Section 69 Clause (2) (c) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

Where the data is transfer from one country to another country, and failure to adhere to cross-border transfer requirement, will attract the high-level penalty.[538]

According to section 70 of this Bill, where any data fiduciary to failure data subject rights such as a request for information on the personal data with the data fiduciary or of request to be "forgotten" is punishable with penalty provide in section 70 of the Bill. According to section 70, punishable with Rs. 5000 per of the default of the subject to a maximum of Rs. 10 Lakh for significant data fiduciary and Rs 5 Lakh for others.[539]

Section 75 of this Bill provide provision related to the "Compensation". According to this section, any data principal who has suffered harm as result of any violation of any provision under this Act, or rules prescribe or regulation specified hereunder, by a data fiduciary or a data processer, shall have right to seek compensation from the data fiduciary.[540]

### 4.29. Appellate Tribunal

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.

According to section 79 of this Bill, Central Government have power to stablish Appellate Tribunal.[541] Appellate Tribunal shall consist of a chairperson and such number of members as may be notified by the Central Government.[542] Establishment of Appellate Tribunal for the fallowing function, that is-

[538] Section 69 Clause (2) (f) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[539] Section 70 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[540] Section 75 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[541] Section 79 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[542] Section 79 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

(a) Hear and dispose of any appeal from an order of the Adjudicating officer under sub -section (5) of section 39

(b) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 65

(c) hear and dispose of an application under sub-section (9) of section 66

(d) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 74

(e) hear and dispose of any appeal from an order of an Adjudicating Officer under subsection (7) of section 75[543]

### 4.29.1. Procedure and power of Appellate Tribunal[544]

According to section 85 of this Bill,

Appellate Tribunal shall not be bound by the procedure laid down the code of Civil Procedure, 1908. But it is guided by the natural justice and subject to other provision of this Act. Appellate Tribunal have power to draft its own procedure.[545] For the discharging its function appellate tribunal have same power as are vested in civil court under the Code of Civil Procedure, 1908.[546]

Where any order passed by the Appellate Tribunal under this Act, deemed as a decree of civil court, and executed as decree. For this purpose, Appellate Tribunal have all the power of a civil court.[547]

### 4.29.2. Appeal to Supreme Court

According to section 87 of this Bill, every appeal against any order of the Appellate Tribunal to the Supreme Court of India.[548] Appeal to the Supreme Court shall be preferred within a period of ninety days from the data of the decision or order.[549] But exceptional circumstances Supreme Court have discretionary power to entertain the appeal after the expiry of said period of ninety days, if supreme court

[543] Section 79 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

[544] Section 85 of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[545] Section 85Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[546] Section 85 Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[547] Section 86 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[548] Section 87 Clause (1) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[549] Section 87 Clause (3) of "The Personal Data Protection Bill, 2018" (Bill of 2018).

satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.[550] But where the decision or order made by the appellate tribunal with the consent of the parties, there shall be no appeal lie against such kind of decision or order.[551]

### 4.30. Offence

Chapter XIII dealt the provision related to the offences.

Offences created under the data protection law should be linked to any intentional or reckless behavior, or to damage caused with knowledge to the data principals in question. Some acts which may be treated as an offence would be:

(i) obtaining, transfer, disclosure and sale of personal and sensitive personal data in violation of the provisions of the data protection law such that it caused harm to the data principal;

(ii) re-identification and processing of previously de-identified personal data.

Such offences may be made cognizable and non- bailable and may be tried by the relevant jurisdictional court.[552]

In cases of offences committed by companies, the person in-charge of the conduct of the business of the company, and in the cases of offences by a government department, the head of the department should be held responsible. However, liability should not be imposed on such persons if they can prove that such offence was committed without her consent or that they put in all reasonable efforts to prevent such commission of an offence.

### 4.31. Conclusions

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

[550] Section 87 Clause (4) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[551] Section 87Clause (2) of "The Personal Data Protection Bill, 2018" (Bill of 2018).
[552] Section 93 of "The Personal Data Protection Bill, 2018" (Bill of 2018).

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" define 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.

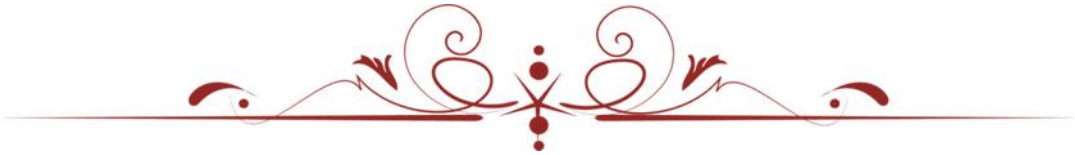
In the "The Data (Privacy and Protection) Bill,2017, provide provision for appeal in limited sense. In this Bill appeal against the decision of the bench, lie to the Telecom Disputes Settlement Appellate Tribunal. Which is set up in accordance with the provision of the Telecom Regulatory Authority Act, 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.

**Suggestions**

The Personal Data Protection Bill,2018 is sufficient for the Data Privacy Protection. It is provided sufficient provision for Data Processing, Data Principals Right, Data Fiduciary Obligations, Appeal to Appellate Tribunal, Appeal to Supreme Court of India, etc. These are sufficient for achieving the objective of this Bill. But some additionally provision are required for the betterment of this Bill, which are suggest by me, that are-

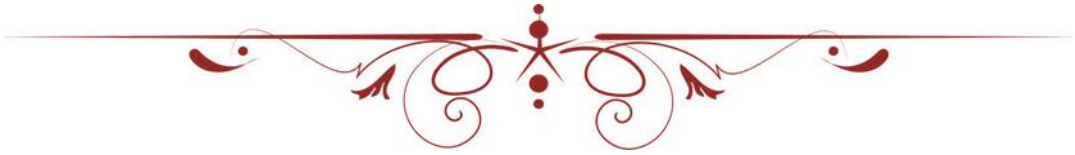
**(a)** Data Principal have "Right to Access" his personal data in this Bill. In this regards time period is not prescribed for this right. In within how much time data fiduciary hand over the brief summary of the processing of personal data or sensitive personal data, to the Data Principal.

**(b)** It is required that the Data Protection Officer, Adjudicating Officers, Appellate Tribunals are stablished in District level for the achieve of the objective of this Bill.



# Chapter V

# Judicial Travelling on the Issue of Privacy and Data Protection



# Chapter V

# Judicial Travelling on the Issue of Privacy and Data Protection

## 5.1. Introduction

The greatest gift to mankind from the scientific community has been the invention of information technology and the associated communication technologies in the last decade of the 20th century. This technology is of such monumental importance that it has been rightly termed as InfoTech revolution. These technologies have put entire human civilization on a fast forward mode by introducing unprecedented speed in information & communication via social media. Social media in particular has greatly impacted political dynamics on a global scale by enabling users to express themselves publicly in ways previously unavailable to them. This very shift in communicative power has spawned greater efforts to restrict and control the use of the internet for information and communication on political, moral, cultural, security and other grounds. This effort of controlling the internet has led to legal and regulatory initiatives to mitigate risks associated with this new medium, ranging from privacy of users, intellectual property, national security, to frauds, pornography and hacking. Regulatory challenges of social media can be broadly addressed under two heads namely.

Today, all democratic societies have come to realize that privacy is at the heart of all human rights. Though, in England there is no constitutional guarantee of human rights against the State, the ordinary law does recognize that an individual has certain rights, such as the right to freedom of speech, to personal liberty and the like which the State would protect against invasion by other persons, in so far as the ambit of such rights is not abridged by legislation. There is, however, no such recognition of any right to privacy as such, in spite forceful advocacy by progressive thinkers such as Lord Denning.

Privacy rights in the United States, Great Britain and India supply an interesting range for comparison because of differences among them in terms of industrial and technological as well as Constitutional development. If the existence of

privacy safeguards depends upon the stimulus provided by some degree of threat, then the legal responses should be greatest in the United States, nearly as great in Britain, and nearly nonexistent in India, because the level of technological and economic development of India, compared to the other two countries does not establish the conditions necessary for the legal safeguard of privacy rights. Privacy as a basic human right touches upon fundamental needs and values associated with man's gregarious nature. Certainly, the level of technological and economic development creates pressures to protect these privacy values through legal enforcement techniques. But even in the absence of such development, the value and the basic human right to privacy may prevail irrespective of legal recognition.

It is true that common law was not able to introduce the right to privacy as an inherent and inalienable right. The American law, however, made a substantial progress in the area of right to privacy. In India we follow the English system of law in its content and procedure. Inherently our courts were not ready to recognize the right to privacy due to the influence of the English Law. But the constitutional provisions are potential enough to introduce the right to privacy by an active judiciary. The issue of right of privacy in India is in premature stage. Hence, an attempt has been made in this chapter to study how far this right can be regarded as constitutional right and the scope is confined to United States of America, United Kingdom and India.

Right to Privacy has been a Customary and a Common Law right, either direct or in indirect manner in the countries of U.S.A., U.K. and India since the ancient period. But, the awareness for the protection of this right has not been there. It is only the modern period, in most of the cases, when the urge for protection of this right has come into being. With the development of society and the establishment of city-lives, people have felt the necessity of Privacy in their personal and family lives.

Moreover, with the advancement of information and communication technology, another aspect of privacy has come into being and that is the protection of computerized personal data of the individuals. In a complex technology-oriented society, we cannot go far without processing the huge amount of computerized personal data, wherein the most serious problem of data theft lies. Data theft creates many serious problems, which include the unauthorized purchasing of personal data

by the direct marketing industries, who us to send us unsolicited direct mails and create direct calls with offers. Apart from that, data theft may be used for creating false identity cards in the name of one using the personal data of others. Prevention of such fraud is very tough and now-a-days countries are using biometric data scanning methods in order to stop the creating of fake identity cards. Therefore, violation of Privacy is mainly of two types – Physical Privacy and Data Privacy.

In fact, there is no direct Constitutional protection of Right to Privacy under the written Constitutions of U.S.A. and India. In the absence of written Constitution, the situation of U.K. is worsening. At this juncture, the Supreme Courts of U.S.A. and India have taken steps for protection of various aspects of Right to Privacy. The courts have interpreted the Constitutional provisions of Bill of Rights or Fundamental Rights in liberal manner in order to incorporate within it, the protection of Right to Privacy. As such, various existing provisions of the U.S. or Indian Constitution have been expanded to include various dimensions of Right to Privacy within themselves. Another problem in this respect is the absence of adequate Privacy protection legislations in all the three countries. Due to this reason, judicial activism and judicial creativity can be the only recourse for protection of Privacy therein. In this respect also, the Supreme Courts of U.S.A. and India as the Human Rights Courts of U.K. have taken active steps. Without the judicial intervention into the matter, the protections of various aspects of Right to Privacy have not been possible in these countries.

### 5.2. Role of Judiciary on the Issue of Privacy and Data Protection in U.S.A.

The Supreme Court of United States has recognized privacy as a constitutional right. In varying contexts, the American judges have found the roots of this right in the First Amendment, the Fourth and Fifth Amendments, in the penumbras of the Bill of Rights and in the Ninth Amendment or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment. Privacy interests of the individual are also protected under the law of torts in United States of America. Evolution of the right to privacy has taken place from case to case development and it appears that the doctrine of “due process of law” has largely helped the American Supreme Court to identify, recognize and protect different kinds of privacy interest.

In ***Boyd v. United States***[553] the Supreme Court recognized privacy as the underlying principle of the Fourth Amendment prohibition against unlawful searches and seizures. Justice Bradley noted the inter-relationship between the Fourth and Fifth Amendments, his significant conclusion was that the purpose of the Fourth Amendment was to protect the security and privacy of "persons, houses, papers, and effects"; as a corollary, police could seize only instrumentalities of a crime but never an individual's papers as mere evidence of a crime. Justice Bradley's conclusion followed from his construction of the reasonableness clause of the amendment. He argued that the individuals have an indefeasible property right at common law and under the Fourth amendment, which renders unreasonable any governmental search and seizure of private papers or other property for mere evidence of a crime. Accordingly, no warrant or subpoena could reasonably issue for items not already owned by or forfeited to the State. In this connection Justice Bradley comments: "The unreasonable searches and seizures condemned in the Fourth Amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the Fifth Amendment.'" Use of the Fourth Amendment as a vehicle for the right of privacy was inhibited in the 1920s because of the heavy reliance placed on it by bootleggers during prohibition. Law is never created in a vacuum, and the interpretation of law, like the making of it, is shaped by the pressures and prejudices of the times.

During the 1920s much "bad" law was written by judges anxious to support the "noble experiment." In particular, Chief Justice Taft narrowed the Fourth Amendment to assist federal agents in keeping America dry." The high point of his fight for prohibition came in the court opinion in ***Olmstead v. United States***.[554] In this landmark case, the majority view expressed by Chief Justice Taft felt that there were essentially property principles underlying the amendment and thus before determining the reasonableness of the search and seizure, it had to be proved that the 'search' involved 'physical trespass' and the 'seizure' included 'tangible material'. Justice Brandeis, however, dissented to give a liberal construction to the amendment. He warned that wiretapping represented a serious threat against privacy under the Fourth Amendment. Had he been heeded by a majority of the court, the most serious invasion

[553] 116 U.S. 616(1886).
[554] 277 U.S. 438 (1927).

against privacy might have been uprooted in its infancy. In the area of traditional searches and seizures, the Supreme Court has had little trouble in recognizing a right of privacy as the underlying interest protected by the Fourth Amendment. With ***Wolf V. Colorado.***[555] the Court extended the federal right against unreasonable search and seizure to the States through the fourteenth amendment. Justice Frankfurter's opinion of the court then recognized "the security of one's privacy against arbitrary intrusion by the police" as being "at the core of the Fourth Amendment" and "therefore implicit in the concept of liberty." Justice Douglas in ***Frank v. Maryland***[556] said, "Indeed, during the last two decades the Fourth Amendment right to be free from unreasonable searches and seizures had become, in shorthand terminology, right to privacy." Wolf was overruled seven years later by ***Mapp v. Ohio,***[557] a decision that clearly equated the fourth amendment with the right of privacy.

In ***Mapp V. Ohio***, the appellant had been convicted of knowingly having in her possession and under control certain lewd and lascivious books, pictures and photographs in violation of Ohio's revised code. The United States Supreme Court held, "Having once recognized that the right to privacy embodied in the Fourth Amendment is enforceable against the States, we can no longer permit that right remain an empty promise. Because it is enforceable, in the same manner and the like effect as other basic rights, secured by the due process clause, we can no longer permit it to be revocable at the whim of any police officer who in the name of the law enforcement itself, chooses to suspend its enjoyment. Our decisions, founded reasons and truth gives to the individual no more than the right which the Constitution guarantees him, to the police officer, no less than that to which honest law enforcement is entitled and to the courts that judicial integrity so necessary in the true administration of justice."

In 1967, the Supreme Court delivered two famous decisions that decisively changed the concept of search and seizure under the fourth Amendment. Physical penetration was no longer necessary to be considered a intrusion. In ***Burger v. New York***[558] conversations recorded by electronic devices in the defendant's office were introduced as evidence in court. The court held that eavesdropping was

[555] 338 U. S. 25 (1949).
[556] 359 U.S. 360 (1959)
[557] 367 U.S. 643(1961).
[558] 388 U.S. 41 (1967)

unconstitutional under the Fourth Amendment. Also, the court found that the New York statute that authorized the bugging was likewise unconstitutional. In ***Katz v. United States***[559]**,** the Supreme Court in 1967 effectively overruled **Olmstead's twin** requirement of a physical trespass or penetration of a constitutionally protected area. In **Katz** federal agents acting without a warrant attached an electronic listening device, similar to a detectaphone, to the outside of a glass public telephone booth in which the defendant was making incriminating calls by relating gambling information. Counsel for the both sides argued the issues of whether the telephone booth was constitutionally protected area in which Katz had a reasonable privacy claim. The Supreme Court held

"*The government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiable relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance."*[560]

The United States Supreme Court in ***Planned Parenthood v. Danforth***[561] held that the Constitution protects a minor's right to privacy to abort her pregnancy. However, the United States Supreme Court's determination to extend the right to privacy protection to encompass a woman's right to abortion was received with heavy criticism by many commentators, because the court declined to recognize during the first trimester the right of the husband to participate in the abortion decision and the interest of the State in protecting the life of the foetus. Further, in an attempt to restrict the scope of constitutionally protected right of abortion the United States Supreme Court in ***Webseter v. Reproductive Health***[562] held that it was legal for the State to prohibit abortion in the State funded public hospitals, and it could also ban publicly paid employees from performing abortions. In 1992, the United States Supreme Court in ***Planned Parenthood of Southern Pennsylvania v. Casey***[563] held that the State is

[559] 389 U.S. 347 (1967)
[560] *Ibid.*
[561] 428 U.S. 52 (1976)
[562] 109 S. Ct 3040 (1989).
[563] 112 S. Ct. 2791(1992).

empowered to impose medic or emotional barriers to abortion, so long as these do not become an undue burden in opting for abortion.

In ***Bowers v. Hardwink***[564] it was held that the State can make homosexualism and sodomy criminal offences without violating the right of privacy. Further, law also prohibits the use of the illegally interception communications if the user knows, or has reason to know, the source. Courts have split the question of whether the first amendment nevertheless enables a party who receives an illegally intercepted communication but was not involved in the interception to disclose the information.

It is, therefore, crystal clear from the foregoing study that the Supreme Court of United States of America has recognized privacy as a constitutional right. The Judges has found the roots of this right in the First, Fourth, fifth amendments in the penumbras of the Bill of Rights and in the Ninth Amendment or in the concept of Hubert guaranteed by the first section of Fourteenth Amendment.

### 5.3. Role of Judiciary on the Issue of Privacy and Data Protection in U.K.

U.K. has continued its conservative and orthodox attitude till the 20th Century and has shown its reluctance to develop Right to Privacy therein. The main reason behind this has been the existence of Unwritten English Common Law, absence of written Constitution and Bill of Rights. The orthodox mentalities of British legislature and British judges have been other reasons for such nonrecognition of Right to Privacy in U.K. In fact, the English legislature and judges have unanimously said since the very beginning that, there has been no general Right to Privacy in U.K. As there has been no written constitution, there has been no question of existence of Constitutional Right to Privacy. What has been available there, has been the existence of Common Law of Torts, which has been used in case of violation of individual right in U.K. In the absence of any written constitution or written laws, it has not been easy to redress the violation of any legal right

In England there is no constitutional guarantee of human rights against the State, the ordinary law does recognize that an individual has certain rights, such as the right to freedom of speech, to personal liberty and the like which the State would

[564] 478 U.S. 186 (1986).

protect against invasion by other persons, in so far as the ambit of such rights is not abridges by legislation.

In the result, law does not protect any unauthorized intrusion into a man's privacy or a disclosure of information regarding a man's private affairs, even though it causes injury or suffering to the person wronged, unless he can establish that such invasion constitutes any one of the recognized torts.

It is crystal clear that there is no general right to privacy under English common law. This has been recognized as a gap in English law, but this is unlikely to change significantly in the near future as United Kingdom governments have been reluctant to introduce such a right. The Government and the U. K. judiciary does, however, believe that the Human Rights Act, 1998 will allow a common law right of privacy to develop.

In the case of ***Wilkinson v. Downton***,[565] a close affinity is found in respect of some aspects between right to privacy and the law of defamation, it is due to the fact that although libel and slander are primarily concerned with reputation, namely, an interest in relation with others. It also safeguards the individuals in the sense of honor and self -respect. But inspite of all that the law of defamation does not confer protection against non-statements which would not constitute wrongful act of defamation but the same would certainly amount to unauthorized exploitation of one's name or reproduction of one's choice of commercial purposes. Similarly, with regard to privacy it was observed as early as the last decade of the nineteenth century that this right should be recognized in favour of the parties in order to preserve their emotional values and to maintain their mental peace and tranquility. There is no doubt that the law recognizes not only the causation of physical injury rather presently it considers it tortuous to cause emotional disturbance and resulting in mental agony to a person. In this regard it has been observed by Warren and Brandeis in their article as under.

***Kaye v. Robertson***[566] where a tabloid journalist ignored notices prohibiting entry to a room where a well-known actor was recovering from extensive head

[565] (1887) 2 Q.B, 57
[566] (1995) 1 WLR 804

injuries, and interviewed and photographed him. An interlocutory injunction was sought on behalf of the action to prevent the paper from publishing the article which claimed that Kaye had agreed to give an exclusive interview to the paper. There being no right to privacy under English law, the plaintiff could not maintain an action for breach of privacy. Justice Glidewell said obiter in that case that there had been a gross invasion of privacy which highlighted a failure in English law. In the absence of such a right of privacy, the claim was based on other rights of action such as libel, malicious falsehood and trespass to the person, in the hope that one or the other would help him protect his privacy. The court expressed its inability to protect the privacy of the individual and blamed the failure of common law and statute to protect this right. However, no cases currently establish such a right although its development has been envisaged.

The right to privacy was recognized in ***Tudc v. Priester***[567] wherein the court prevented the defendant who was required to make copies of the picture belonging to the plaintiff by keeping copies of the picture and selling such copies to the customers. The court held that the plaintiff was entitled to get injunction as well as damages for the breach of contract. Similarly, in the case of ***Pollard v. Photographic Co***[568]. a photographer was restrained from exhibiting a photograph of a lady and selling the copies of the photograph, on the ground that it was breach of contract as well as confidence.

The right to privacy was also protected in the case of ***Prince Albert V. Strange***[569] wherein the common law rules prohibited not merely the reproduction of etching made by the Prince Albert and Queen Victoria or their private amusement. The etching, which represented members of the Royal family and matters of personal interest, were entrusted to a printer for making impressions. An employee of the printer made unauthorized copies and sold them to the defendant who in turn proposed to exhibit them publicly. Prince Albert succeeding in obtaining injunction to prevent the exhibition. The Court's reasoning was based on both the enforcement of the Prince's property rights as well as the employee's breach of confidence.

[567] 19 Q.B.D
[568] 40 Ch. D 345 (1888).
[569] 41 ER 1171 (1849

## 5.3. Role of Judiciary on the Issue of Privacy and Data Protection in India

The 'data protection' and 'right to privacy' has much more similar to each other. The 'data protection' can only be possible if the encroachment of privacy is being stopped. Privacy law in general, and informational privacy in particular, have always been closely linked to technological development.[570] In their seminal 1890 article 'The Right to Privacy', Warren and Brandeis lament the 'instantaneous photographs and newspaper enterprise that have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops".[571] This is the genesis of the privacy matter. Now a days this is being developed in 'data protection'. The idea of 'Data Protection' has its different aspects. The different aspects of data protection as a right like, the right of access to data banks, the right to check their exactness, the right to bring them up to date and to correct them, the right to the secrecy of sensitive data, the right to authorize their dissemination: all these rights together today constitute the new right to privacy.[572] Hence in this matter the linkage of 'Data Protection' and 'Privacy' status are very much appropriate as a right based approach.

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.

Judiciary in India enjoys a very significant position since it has been made the guardian and Custodian of the Constitution. It is not only a watch dog against violation of fundamental rights guaranteed under the Constitution but protects all

[570] Graham Greenleaf and Sinta Dewi Rosadi, "Indonesia's data protection Regulation 2012: A brief code with data breach notification," Privacy Laws & Business International Report, Issue 122, (2013): 24-27

[571] Praveen Dalal, "Data Protection laws in India: A Constitutional Perspective," Accessed October 21, 2016
http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-ININDIA.pdf

[572] I. N. Walden and R. N. Savage, "Data Protection and Privacy Laws: Should Organizations Be Protected" The International and Comparative Law Quarterly, Vol. 37, No. 2 (1988): 337-347.

persons, Indian and aliens alike, against discrimination, abuse of state power, arbitrariness etc. Liberty and Equality have well survived and thrived in India due to the pro-active role played by the Indian Judiciary. The Supreme Court has, over the years, elaborated the scope of fundamental rights. Upholding the rights and dignity of individual, in true spirit of good governance.

In our country the sole credit goes to the Judiciary for recognizing the concept of privacy because neither the constitution nor any other statute in our country defined this concept. Still a lot more has to be done for the recognition and protection of privacy by law in 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***[573] 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.

Article 19(1) (a) stipulates that "all citizens shall have the right to freedom of speech and expression". However, this is qualified by Article 19(2) which states 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

[573] 2017(10) SCALE 1

the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence". Thus, the freedom of expression guaranteed by Article 19(1) (a) is not absolute, but a qualified right that is susceptible, under the Constitutional scheme, to being curtailed under specified conditions.

Article 21 reads "No person shall be deprived of his life or personal liberty except according to procedure established by law." Article 21 only requires a "procedure established by law" as a pre-condition for the deprivation of life and liberty.

Recently in case of ***Justice K. S. Puttaswamy (Ret.) and Others Vs. Union of India and Others***[574] 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".

In ***Nihal Chand v. Mt. Bhagwan Devi***[575], Allahabad High Court took first step when it recognized an independent existence of the right to privacy as emerging from the custom and traditions of the people besides being a statutory right, the court observed:

"*The right to privacy based on social custom is different from a right to privacy based on natural modesty and human morality. The latter is not confined to any class, creed, color or race. It is a birth right of any human being and is sacred and should be observed. This right should not be exercised in an oppressive way."*

The movement towards the recognition of right to privacy in India started with ***Kharak Singh vs The State of U.P***.[576] 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.

[574] 2017(10) SCALE 1
[575] AIR 1935 All 1002.
[576] AIR 1963 SC 1295

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.

### 5.4.1. Phone Tapping and Privacy

In 1972, the Supreme Court decided a case — one of the first of its kind on wiretapping. In ***R. M. Malkani vs State of Maharashtra***[577] 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."

In this case, the telephonic conversation between two parties was tape-recorded by the police with the consent of one of the parties. The Supreme Court observed that the conversation could be used in evidence as it was voluntary and there was no duress or compulsion to extract the same. The fact that the tape-recording instrument was attached without appellant's knowledge does not make the conversation inadmissible against him. The Supreme Court further observed that it would not tolerate safeguards for the protection of citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods. At the same time the court held that even stolen evidence was admissible if it was not tainted by an inadmissible confess of guilt.[578]

[577] AIR 1973 SC 157
[578] AIR 1973 SC 157

In ***Yusuf Ali Ismail Nagree v. State of Maharashtra***[579] the court was faced with the question whether tapping of the appellant's conversation without his knowledge offended his right under Article 21. In this case, the police inspector tapped the conversation between Nagree and Sheikh, a municipal clerk whom Nagree wanted to bribe. Nagree had no knowledge of this. Nagree challenged the admissibility of such evidence. The court evolved two directions for guidance in admitting such evidence.

It said Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. The telephonic conversation of an innocent citizen would be protected by courts against wrongful or highhanded interference by tapping the conversation. The protection is not for a guilty citizen against the efforts of police to vindicate the law and prevent corruption in public servants. It must not be understood that the courts would tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods.

In the case of ***PUCL vs. Union of India***[580] 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 held: 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.

In ***Smt. Rayala M. Bhuvaneshwari v. Nagaphanender Royals***[581], the court observed that:

[579] AIR 1973 SC 15
[580] AIR 1997 SC 568

"The act of Tapping by the husband of conversation of his wife with other without her knowledge was illegal and amounted to infringement of her right to privacy under Article 21 of the constitution. These talks even if true cannot be admissible in evidence. The wife cannot be forced to undergo voice test and then asked the expert to compare portion denied by her with admitted voice. The court observed that the purity of the relation between husband wife is the basis of marriage. The husband was recording her conversation on telephone with her friends and parents in India without her knowledge. This is clear infringement of right to privacy of the wife. If husband is of such a nature and has not faith in her wife even about her conversations to her parents, then the institution of marriage itself becomes redundant."

In ***Directorate of Revenue v. Mohammad Nisar Husain*** [582], the court observed that,

"That an authority cannot be given an untrammeled power to infringe the right of privacy of any person. Even if a Statute confers such powers upon an authority to make search and seizure of a person at all hours and at all places, the same may be held ultra-virus unless the restriction imposed are reasonable one, what would be reasonable restrictions would depend upon the nature of the statute and extent of the right sought to be protected. Although a statutory power to make a search and seizure by itself may not offend the right of privacy in a case of this nature. The least that a court can do is to see that such a right is not unnecessarily infringed right to privacy deals with person not places."

"If he does not break a law would be entitled to enjoy his life and liberty which would include the right not to be disturbed. A right to be let alone is recognized to be a right which would fall under Article 21 of the Constitution of India."

In ***State of Maharashtra v. Bharat Shanti Lal Shah***[583], the Supreme Court said that interception of conversation though constitutes an invasion of an individual's right to privacy but right can be curtailed in accordance with procedure validly established by law. Court has to see that the procedure itself must be fair, just and

[581] AIR 2008 A P 98.
[582] AIR 2008 SC 524.
[583] (2008) 13 SCC 5.

reasonable and not arbitrary, fanciful or oppressive. An authority cannot be given an untrammeled power to infringe the right to privacy of any person.

In case of ***Amar Singh v Union of India***[584], the Hon'ble Supreme Court while dealing with allegation of beach of fundamental right to privacy relating to telephone interception, imposed "a kind of duty to care" upon non-State service providers and held that "service provider has to act as a responsible agency and cannot act on any communication". The Hon'ble Supreme Court further held that "Act immediately but verify simultaneously".

### 5.4.2. Surveillance and Privacy

Further in ***Govind vs. State of Madhya Pradesh***[585] 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 **this case** [586], the Supreme Court of India developed the law of privacy by holding that domiciliary visit of the police and disclosure of the information. These disclosures of the information approaching the modern data protection concern.

In ***Malak Singh v. State of Punjab & Haryana***[587] the court held that:

"While exercising surveillance over reputed bad characters, habitual offenders, and potential offenders the police should not encroach upon the privacy of a citizen so as to offend his right under Article 21 and Article 19(l)(d) of the constitution."

[584] (2011) 7 SCC 69
[585] (1975)2 SCC 148
[586] AIR 1975 SC 1378.
[587] AIR 1981 SC 760.

### 5.4.3. Freedom of Speech and Expression and Privacy

In ***R. Rajagopal v. State of Tamil Nadu***[588] known as "Auto Shankar Case"

In this 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. The case related to the alleged autobiography of Auto Shankar who was convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various police officials

In this case the petitioner was the editor, printer and publisher of a Tamil weekly magazine published in Madras who sought an order restraining the State of Tamil Nadu from interfering with the authorized publication of the autobiography of Auto Shankar, a condemned prisoner awaiting the death penalty which was based on public records. In this case Jeevan Reddy, J reaffirmed that the right to privacy is implicit in the right to life and liberty guaranteed in Article 21 of the Constitution. The Court also affirmed that the 'right to be let alone' for every citizen of this country to safeguard their privacy.

Supreme Court held that:

*"The 'right to privacy' or the 'right to be let alone' is guaranteed by Article 21 of the constitution. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and 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. If he does so, he would be violating the right of the person concerned and would be liable in an action for damages. However, position may be differed if he voluntarily puts into controversy or voluntarily invites or raised a controversy."*

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

[588] AIR 1995 SC 264.

concerning the above matters without his consent- whether truthful or otherwise and whether laudatory or critical

### 5.4.4. Gender Priority on Privacy

In ***T. Sareetha v. T. V. Subbaish***[589] The Andhra Pradesh High Court Observed that,

*"Sexual cohabitation is an inseparable ingredient of a decree for restitution of conjugal rights the purpose of the decree is to force the party to behave and act as husband or wife with the other party which includes the duty to have sex also and in case of wife, even against her will and consent. The decree terminates the choice to have or not to have the sex and the choice to allow or not to allow one's body to be used as a vehicle for another human being. Thus, it offends the inviolability of body and mind and offends the integrity of wife and invades her marital privacy and domestic intimacies. The court further observed that nothing can conceivably be more degrading to human dignity and monstrous to human spirit than to subject a person by a long arm of the law to a positive sex act."*

Chaudhary J. stated that it cannot be admitted that a decree for restitution of conjugal rights constitutes the grossest form of violation of an individual's right to privacy. The right to privacy guaranteed by Article 21 is flagrantly violated by the decree.

***State of Maharashtra v. Madhuker Narayan Markikar***,[590] Suprem Court held that,

*"The 'right to privacy' is available even to a woman of easy virtue and no one can invade her privacy. A police inspector visited the house in uniform and demanded to have sexual intercourse with her. On refusing he tried to have her by force. She raised a hue and cry. When he was prosecuted, he told the court that she was a lady of easy virtue and therefore her evidence was not to be relied. The court rejected the argument of the applicant and held him liable for violating her right to privacy under Article 21 of the constitution."*

[589] AIR 1983 AP 356.
[590] AIR 1991 SC 207.

The right to privacy implies the right not merely to prevent the incorrect portrayal of private life but the right to prevent it being depicted at all. Even a woman of easy virtue is entitled to privacy and no one can invade her privacy as and when he likes.

***Neera Mathur v. LIC of India,***[591] court held that, modesty and self-respect may perhaps preclude the disclosure of such personal problems like whether her menstrual period is regular or painless etc.

In the case of ***State of Punjab v. Baldev Singh***[592] court held that, the basic right of female is to be treated with decency and proper dignity. But if a person does not like marriage and lives with another the society should be able to permit it. Sense of dignity is a trait not belonging to society ladies only, but also to prostitutes.

In ***State of Karnataka v. Krishnappa***[593], the court strengthened the protection of the right to privacy over the person by requiring stem punishment of rapists. The offence was held to be seriously violating the right to privacy Sexual violence apart from being a dehumanizing act is an unlawful intrusion of the right to privacy and sanctity of a female. It is a serious blow to her supreme honors and offends her self-esteem and dignity. It degrades and humiliates the victim and where the victim is helpless innocent child, it leaves behind a traumatic experience. The Court are therefore, expected to deal with cases of sexual crime against woman with utmost sensitivity. Such cases need to be dealt with sternly and severely.

In ***Vandna Kumari v. P Praveen Kumar***[594], husband filed a petition under Section 12(1) (d) of the Hindu Marriage Act. Praying for a decree of nullity four months after the solemnization of marriage on the ground that at the time of marriage his wife was pregnant by a person other than him and he was unaware of it. She thus was guilty of this extreme fraud and he should be granted a decree of nullity. He further contended that the marriage was not consummated, and as a proof of his allegation, he sought a DNA test to be performed on the wife and the foetus. The wife contested his allegation and also the plea for the DNA test on the ground, these tests

[591] AIR 1992 SC 392.
[592] AIR 1999 SC 2378.
[593] AIR 2000 SC 1470.
[594] AIR 2007 AP 17.

were unnecessary as legitimacy of the child was not in question and the same would also amount to a violation of her rights of privacy. The trial court held that it was a fit case for the order of DNA test, and directed the wife to undergo this test. The wife preferred an appeal. The High Court held that though the issue directly was not with respect to the legitimacy of the child, but indirectly the husband would be deemed to be the father of the child if no access at the time of the possible conception cannot be proved.

### 5.4.5. Health and privacy

In ***Mr. 'X'. Vs. Hospital Z***[595] is unique in this area due to the strange nature of its fact. This case is similar to Raj Gopal's case only to the extent that both involved public disclosure of private facts. The facts and nature of the cases are entirely different. The Supreme Court has held that although the "right to privacy" is a fundamental right under Article 21 of the Constitution but it is not an absolute right and restrictions can be imposed on it for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others.

In ***Selvi v. State of Karnataka***[596]. , the Supreme Court held that the right of privacy to hold these technologies unconstitutional.

"Even though these are non- invasive techniques the concern is not so much with the manner in which they are conducted but the consequences for the individuals who undergo the same. The use of techniques such as 'Brain Fingerprinting' and 'FMRI-based Lie-Detection' raise numerous concerns such as those of protecting mental privacy and the harms that may arise from inferences made about the subject's truthfulness or familiarity with the facts of a crime."

Further down, the court held that such techniques invaded the accused's mental privacy which was an integral aspect of their personal liberty.

In **this case** [597] the decision made by the Supreme Court of India is strikingly indicated that the American doctrine of due process has firmly become a part of

[595] AIR 1999 SC 495.
[596] (2010) 7 SCC 283.
[597] (2010) 7 SCC 283.

Indian Constitutional Law, despite the Constitution -framers' contrary intentions. In this case Chief justice K.G Balakrishnan held that:

"*The 'Substantive due process' is now a 'guarantee' under the Constitution. This declaration is a remarkable rejection of the framers' decision to delete the due process clause. In its narcoanalysis opinion, the court upheld a right to mental privacy, recognizing an 'unenumerated' right as American courts would in exercise of the due process clause."*

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 in to personal liberty. Forcible interference with a person's mental processes is not provided under any statute and it most certainly comes in to conflict with the right against self-incrimination.

***Sarda v. Dharmpal***,[598] and ***Bhabani Prasad Jena v. Orissa State Commission for Women***[599] court held that, If DNA test is eminently needed to reach the truth, the Court must exercise the dissector of medical examination of a person.

**Woman Reproductive choice and Privacy**

In ***Suchitra Srivastava and another's v. Chandigarh Administration***[600], the Court observed:

"When the MTP Act was first enacted in 1971 it was largely modeled on the Abortion Act of 1967 which has been passed in the United Kingdom. The legislative intent was to provide a 'qualified right to abortion' and the termination of pregnancy has never been recognized as a normal recourse for expecting mothers. There is no doubt that a woman's right to make reproductive choices is also a dimension of personal liberty as understood under Article 21 of the Constitution of India. It is important to recognize that reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a women's right to privacy, dignity and bodily integrity should be respected."

[598] AIR 2003 SC 3450.
[599] (2010)8 SCC 633.
[600] (2009) 9 SCC 1.

### 5.4.7. Search and Seizure Vs. Privacy

In a case ***M.P Sharma v. Satish Chandra***[601], Supreme Court held that the contention that search and seizure violated Article 19(1) (f) of the Constitution. The Court took the view that a mere search by itself did not affect any right to property, and though seizure affected it, such effect was only temporary and was a reasonable restriction on the right to privacy. Then the right to privacy has been developed in the Constitutional sphere of India under the Article 19 (1) (a) and Article 21.

However, the Right to Information Act isn't as convenient a vehicle for privacy abuse as this case may suggest. The RTI adjudicatory apparatus has on several occasions upheld the denial of information on grounds of privacy violation.

In ***Board of Revenue, Madras v. R. S. Jhawar***[602], the Supreme Court held that the power of search and seizure can be exercised by an administrative authority only when it is conferred on it by a statute. The stipulations made by the statutes in question regulating the power of search and seizure must be observed by the authority concerned, otherwise search and seizure will be declared illegal and nothing recovered at such a search can be made use of an evidence against the individual concerned.

In ***V.S. Kuttan Pillai v. Ramakrishna***[603] the court held that: "General warrant for searching and seizing listed documents would not entail invasion of privacy even if the search did not yield any result because of countervailing State interests. "

In ***State of Punjab v. Baldeo Singh***[604], the court held that:

"For a search of a person the safeguards provided under Section 50 of the Code of Criminal Procedure are mandatory to be followed. The invasion of a person has been given a protection through insistence on a procedural safeguard but the court has not ruled that evidence obtained in breach of Section 50 safeguards would be impermissible evidence."

[601] AIR 1954 SCR 1077.
[602] AIR 1968 SC 59.
[603] AIR 1980 SC 185.
[604] AIR 1999 SC 2378

The most significant development outside search and surveillance issues is the hew decision of the High Court of Delhi, In the ***Naz Foundation v. Government of NCT of Delhi*** the case was public interest litigation brought by the NGO, Naz Foundation challenging the Constitutional validity of Section 377 of the Indian Penal Code, 1860.

The petitioners argued 'to the effect that the prohibition of certain private, consensual sexual relations (homosexual) provided by Section 377 IPC unreasonably abridges the right of privacy and dignity within the ambit of right to life and liberty under Article 21, which can be abridged only for a compelling state interest which, in its submission, is amiss here'.

The observation of the Court holding that Section377 breached the right of privacy is as follows:

"The sphere of privacy allows persons to develop human relations without interference from the outside community or from the State. The exercise of autonomy enables an individual to attain fulfillment, grow in self-esteem, build relationships of his or her choice and fulfill all legitimate goals that he or she may set. In the Indian Constitution, the right to live with dignity and the right of privacy both are recognized as dimensions of Article 21. Section 377 IPC denies a person's dignity and criminalizes his or her core identity solely on account of his or her sexuality and thus violates Article 21 of the Constitution, as it stands. Section 377 IPC denies a gay person a right to full personhood which is implicit in notion of life under Article 21 of the Constitution."

### 5.4.8. Data Protection and Privacy

In Case of ***District Registrar and Collector, Hyderabad v. Canara Bank***[605] the Supreme Court contended that the search and seizure by the enforcement agency of any registers, books, records, papers, documents or other proceedings for the purpose of collecting evidence and discovering the fraud and omission of stamp duty payable or not of an individuals are come under the infringement situation, secrecy and confidentiality must be maintain.

[605] AIR 2005 SC 186.

In the case of ***Vijay Prakash v. Union of India***[606], the Delhi High Court has held that, service records and information of the Public Servants would amount to their private and personal information; as such, those information's could not be claimed to disclose for seeking Right to Information. Accordingly, it has been held that, those information's would amount to be the private information's of the Public Servants and disclosure of such information's would amount to serious violation of their Right to Privacy. As such, without stating the gross violation of public interest, such information's could not be disclosed for seeking the Right to Information.

In an interesting case ***Mr. Ansari Masood A.K v. Ministry of External Affairs***[607], the Central Information Commission has held that "details of a passport are readily made available by any individual in a number of instances, example to travel agents, at airline counters, and whenever proof of residence for telephone connections etc. is required. For this reason, disclosure of details of a passport cannot be considered as causing unwarranted invasion of the privacy of an individual and, therefore, is not exempted from disclosure under Section 8(l)(j) of the RTI Act." This is despite the fact that nothing in the Passport Act itself authorizes disclosure of any documents under any circumstances.

In a case of ***Ram Jethmalani & Others v. Union of India***,[608] held that

"Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner. Revelation of bank account details of individuals, without establishment of prima facie grounds to accuse them of wrong doing, would be a violation of their rights to privacy. State cannot compel citizens to reveal, or itself reveal details of their bank accounts to the public at large, either to receive benefits from the State or to facilitate investigations, and prosecutions of such individuals, unless the State itself has, through properly conducted investigations, within the four corners of constitutional permissibility."

Recently, this issue was once again raised before the Hon'ble Supreme Court in the case of ***K. S. Puttaswamy (Retd.) v Union of India***[609], in which case the

[606] AIR 2010 Delhi 7.
[607] (2010) 9 SCC 152.
[608] (2011) 8 SCC 1.

'**Aadhaar Card Scheme'** was challenged on the ground that collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is in breach of the fundamental right to privacy embodied in Article 21 of the Constitution of India. Given the ambiguity from prior judicial precedents on the constitutional status of right to privacy, the Hon'ble Supreme Court referred the matter to a constitutional bench consisting of nine judges.

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

The primary Defence of the Union of India was that

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

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

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

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

The Hon'ble Supreme Court by its decision pronounced on August 24, 2017 unanimously held a that,

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

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

[609] 2017(10) SCALE 1

(iii)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.

(iv)Decisions subsequent to Kharak Singh which have enunciated the position in (iii) above lay down the correct position in law."

Hon'ble Mr. Justice D.Y. Chandrachud, clearly held that: -

(A) Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian Constitution.[610]

(C) Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III.[611]

(F) Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognizes the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognizes the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being.[612]

(H) Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the

[610] Ibid. para 3(A).
[611] Ibid. para 3(C).
[612] Ibid. para 3(F).

touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of

(i) legality, which postulates the existence of law;

(ii) need, defined in terms of a legitimate state aim; and

(iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.[613]

(I) Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.[614]

The Hon'ble Supreme Court rejected the arguments of the Union of India, and while analyzing the nature of right of privacy as regards its origin[615], the Hon'ble Supreme Court held that the right to privacy is intrinsic to and inseparable from human element in human being and core of human dignity[616]. Thus, it was held that privacy has both positive and negative content. The negative content acts as an embargo on the State from committing an intrusion upon the life and personal liberty of a citizen and its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual[617]. Therefore, the constitutional protection of privacy may give rise to two inter-related protections i.e.

(i) Against world at large, to be respected by all including State: right to choose that what personal information is to be released into the public space

[613] Ibid. para 3(H).
[614] Ibid. para 3(I).
[615] Ibid, para 53-65, 531-536, 718, 73.
[616] Ibid, Para 459.
[617] Ibid, Para 403.

(ii) Against the State: as necessary concomitant of democratic values, limited government and limitation on power of State[618].

As a result of this judgment the right to privacy has become 'more than mere common law right' and 'more robust and sacrosanct' than just any statutory right. Thus, now in the context of Article 21 of the Constitution, an invasion of privacy must be justified on the basis of 'a law' which stipulates a procedure which is fair, just and reasonable. It is to be noted that since ***R.C. Cooper v UOI***[619], 'procedure established by law' in Article 21 has gained substantive due process element as well [620] whereby even the contents of the law can be challenged being not in accordance with requirements of a valid law. Therefore, because of right of privacy being recognized as fundamental right, existing sectoral legislations, if challenged, may now have to pass the rigors of aforesaid test. Same would not have been the position, if privacy would have remained mere statutory or common law right.

As a consequence, now the "Aadhaar Card Scheme" which was alleged to be in breach of fundamental right to privacy, will now be tested by the same standards by which a law which invades personal liberty under Article 21 is liable to be tested.

While discussing the right to information privacy in today's world, the Hon'ble Mr. Justice D.Y. Chandrachud concluded as[621] -

(1) "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.

(2) "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

[618] Ibid, Para 304-307.
[619] (1970) 1 SCC 248.
[620] Mohd. Arif vs. Registrar, Supreme Court of India, (2014) 9 SCC 714.
[621] 2017(10) SCALE 1

information, which an individual may not want to give, needs the protection of privacy."

(3) "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."

**Conclusions**

In view of the above propositions we may safely conclude 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***.[622] 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.

[622] AIR 1963 SC 1295

In 1972, the Supreme Court, In ***R. M. Malkani vs State of Maharashtra***[623] 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***[624] 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***[625]**.** 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

[623] AIR 1973 SC 157
[624] (1975)2 SCC 148
[625] (1994)6 SCC 632

In the case of ***PUCL vs. Union of India***[626] 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.

In ***X. Vs. Hospital Z***, The Supreme Court was confronted with the test of striking a balance between two conflicting fundamental rights: the Aids patients right to life which included his right to privacy and confidentiality of his medical condition, and the right of the lady to whom he was engaged to lead to healthy life. Supreme Court held that right to privacy is an essential component of right to life but it is not absolute and may be restricted for the prevention of crime, disorder or protection of health or morals or for the purpose of protection of rights and freedom of others.

The most significant development in respect of protection of privacy is the recent decision of the High Court of Delhi in the ***Naz Foundation Case***, in which the Court held that Section 377 of the Indian penal code violated Articles 21, 14 and 15 of the Constitution, insofar as it criminalizes consensual sexual acts of adults in private. Because of the doctrine of severability, it 'will continue to govern non-consensual penile non-vaginal sex and penile nonvaginal sex involving minors. Right to privacy in respect of abortion is another such area which has not discussed in any Indian legislation.

Recently in ***Suchitra Srivastava and others v. Chandigarh Administration*** the Supreme Court observed that, there is no doubt that a woman's right to make reproductive choices is also a dimension of personal liberty as understood under Article 21 of the Constitution of India. It is important to recognize that reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a women's right to privacy, dignity and bodily integrity should be respected.

[626] AIR 1997 SC 568

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***[627] 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***[628] 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."*

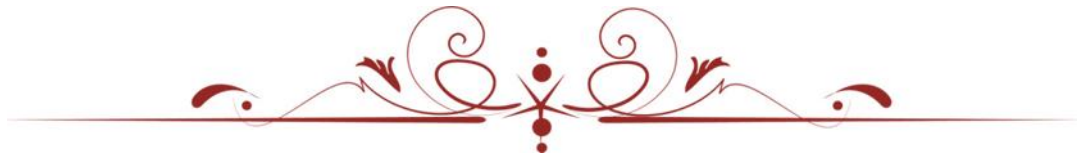
For this Purpose, Government of India has set up Committee of Experts to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill. The objective is to

[627] 2017(10) SCALE 1
[628] 2017(10) SCALE 1

"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.

To conclude the right to Data Privacy in India as in any other jurisdiction, though not statutorily codified as yet. Its scope is by the lack of such a codification neither extremely narrow nor considerably wide. This implies that this aspect should be handled with a great deal of care and circumspection.



# Chapter VI

# Reporting Research Findings

# Chapter VI
# Reporting Research Findings

## 6.1. Introduction

Facebook, LinkedIn, and Twitter distribute their social APIs far developers to integrate with their websites. It is at this point where the transfer of data happens. After a user is authenticated via social login, the APIs will expose personal data such as name, gender, email and physical location. LinkedIn further exposes other identifiable data such as job, your professional career networks, which will also expose the people inside that network.

Security concern is another matter. With malicious social apps, clickjacking, and thefts of accounts, there is every chance that shared content carry unfortunate side effects. While existing web filters and corporate anti-virus will help, it still addresses the endpoint security. Some web-based endpoint web filters can intercept traffic after encryption. That means, even though social sites provide SSL connection at the point of authenticating users, there is still a chance of eavesdropping, in particular if a user is accessing the sites via their own mobile phones or tablets.

With cloud computing and SNS, data can reside in any data center located in various parts of the world. Where data are strongly encrypted and the decryption keys securely managed, the data location should be irrelevant.

In India this is big problem. In India lot of people use internet, SNSs, social media, etc in their daily life, but they but they don't know about their data user rights, what is Sensitive personal Data, what is provision provided in Data Protection Bill, 2018, when breach their data privacy what remedies available and where they go for remedies, etc. These problems are arising in India for the protection on data privacy. Put in minds these problem researchers put "Chapter VI- Finding of Non-Doctrinal Case Method" in their research topic. In this chapter researcher collect data and analysis that data. In this analysis researcher want to 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. In questionnaire, first question is that,"Do you use internet?"

Regarding this question out of 205-people, 200 people response that they are use internet, while 05 person accept that they are not use internet. Its show in chart 1.

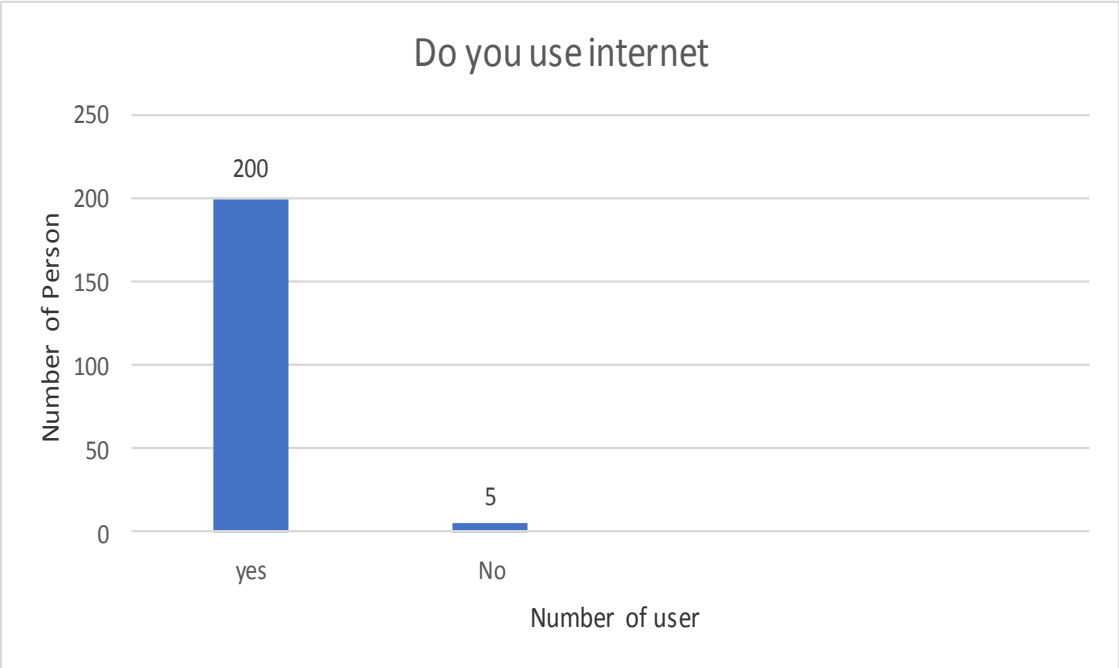



**Chart 1**

According to chart 1, it is analysis that the maximum number of people use the internet. Approximate 98% people use internet in their daily life. It is the need for our daily life. Our maximum activity related to our progressive life is drive by the internet. Its play a vital role in our daily life. In my questionnaire my next question is that,"Do you know about how to use internet?"

Regarding this question out of 200-person, 150-person response yes, 30-person response No, and 20- persons response to know some extent. Its show on chart 2.

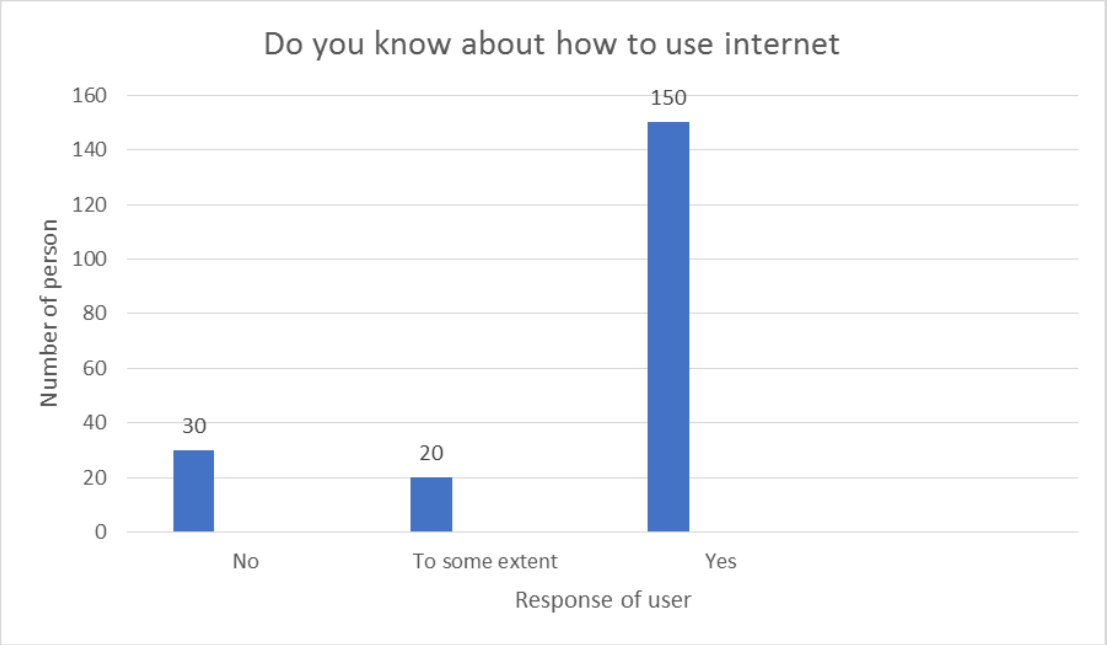



**Chart 2**

According to chart 2, 200 people use internet, but in 200 people only 150 people know how to use internet. 30 people have no knowledge to how to use internet, 20 people have to some extent knowledge that how to use internet. According to this chart approximate 75% people have knowledge that how to use internet, but 15% have no knowledge that how to use internet, and 10% people have some extent knowledge that how to use internet. In my questionnaire next question is that, "For what purpose do you use internet? For this question chart 3 provided some useful data. Regarding this question, according to chart 3,

125 people response that they are use internet for information, 169 people use internet for send and receive E-mails, 142 people use for social networking sites, 86 people use for Professional issue, 67 people use for gaming, 96 people use for instant messaging, 85 people use internet for sharing photos and videos, 110 people use for social media, 115 people use for educational purpose, 90 people use for online shopping, 57 people use for entertain purpose, 64 people use for download music and videos, and 58 people response that they are use internet for other purpose also.

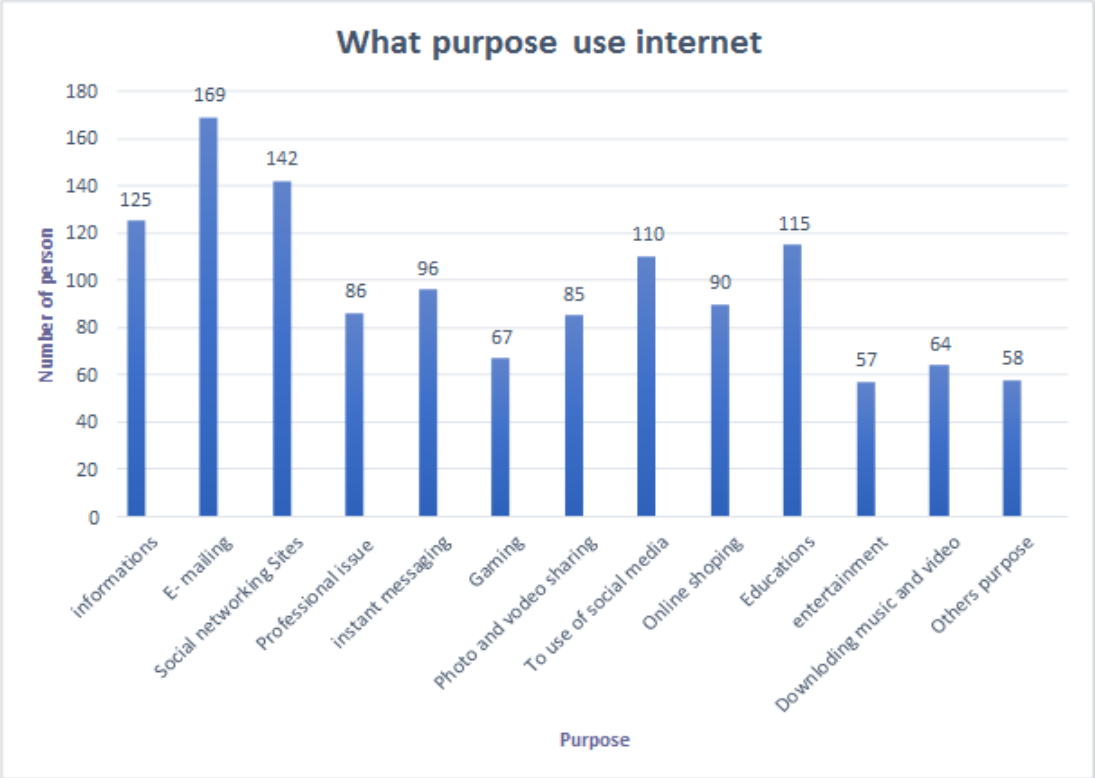



**Chart 3**

According to chart 1, chart 2, chart 3, researcher analysis that approximate 98% people use internet (see in chart 1) for different purpose (see in chart 3) but only approximate 75% people have knowledge that how to use internet. Approximate 15% people don't have knowledge that how to use internet. That is adversely affected the data privacy. In the questionnaire next question is that, "Do you have an account on social networking sites?" In this regard, according to chart 4,

190 people out of 200 people response that they have an account on social networking sites. While 10 people out of 200 responses that they have no any account on social networking sites. It means approximate 95 % internet user have account on social networking sites. While 5% people don't have account on social networking sites.

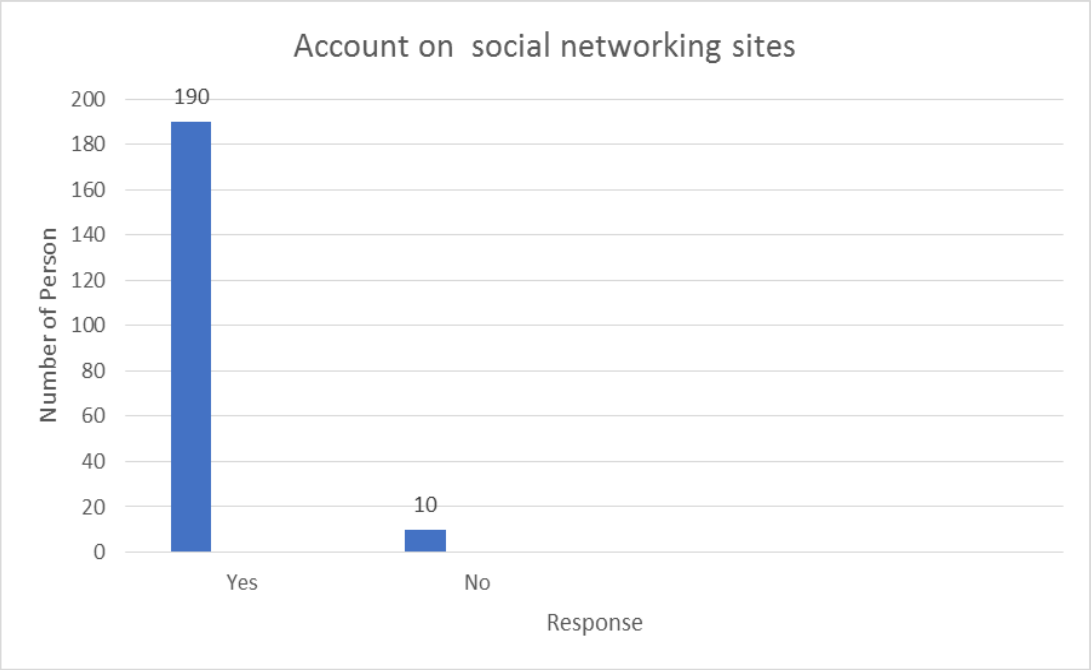



**Chart 4**

In the questionnaire next question is that, "How did you come to know about Social networking sites?" Regarding this question chart 5 prepared on the basis of data collections.

According to chart 5, 117 peoples out of 200 response that they are known about social networking by self. While 38 people response that they are known by their friends, and 45 people are known that by their family.

It means approximate 58 % people know about social networking sites by self, while 19% people know about social networking sites by their friends and 23 % people by their family.

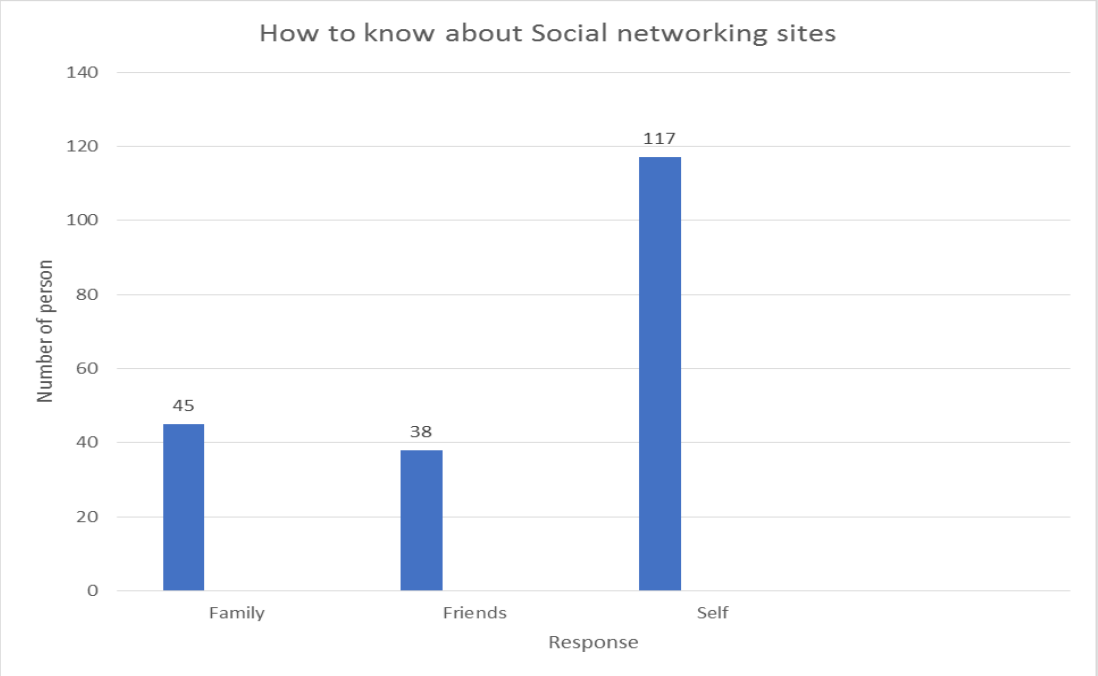



**Chart 5**

According to chart 5, 117 peoples out of 200 response that they are known about social networking by self. While 38 people response that they are known by their friends, and 45 people are known that by their family. In questionnaire next question is that, "How frequently do you use Social networking sites?" In this regard researcher prepared chart 6.

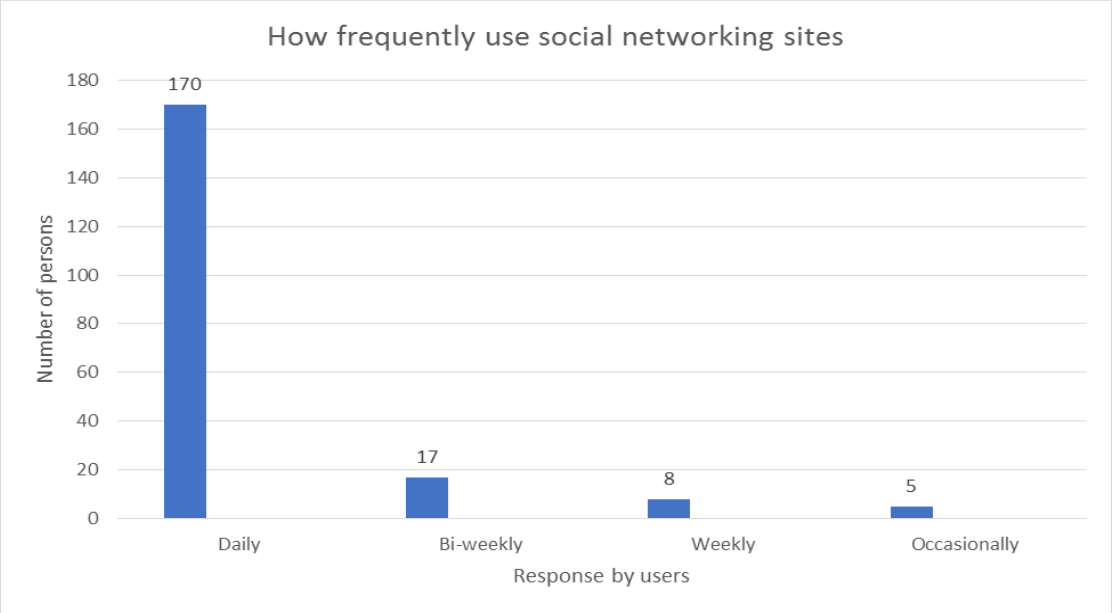



**Chart 6**

According to chart 6, 170 people out of 200 response that they are use social networking sites daily, while 17 people out of 200 response that they are use social networking sites Bi-weekly, 8 people use social networking sites weekly and 5 people use social networking sites Occasionally.

According to chart 6, Its cleared that, approximate 85 % people use social networking sites daily. It means maximum person use social networking sites for their progressive life. They use social networking sites for information, send and receive mail, share photo and videos, for entertainment, etc. while approximate 8 % people use social networking sites Bi-weekly, 4 % people use social networking sites weekly, and 3 % people use social networking sites occasionally. In the questionnaire next question is that, "How much time do you spend on social networking sites?" In this regards research prepared the pie chat 7 on the basis of collected data.

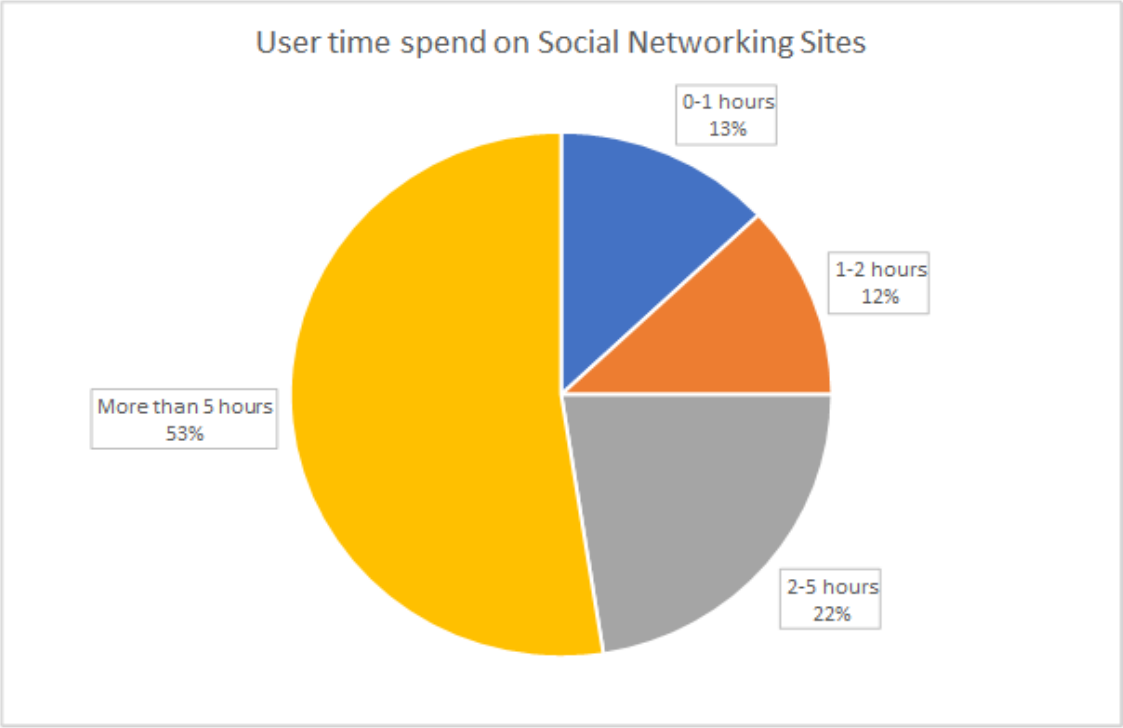



**Chart 7**

According to chart 7, 53 % people use social networking sites (SNSs) more than 5 hours daily. 22 % people use SNSs 2-5 hours daily, while 12 % people use SNSs 1-2 hours daily and 13 % people use SNSs 0-1 hours daily. It means maximum people spend much time on social networking sites but they not aware about their data

privacy. In the questionnaire next question is that, "Which Social Networking Sites you access?" In this regard's researcher prepares the chart on the basis of collected data.

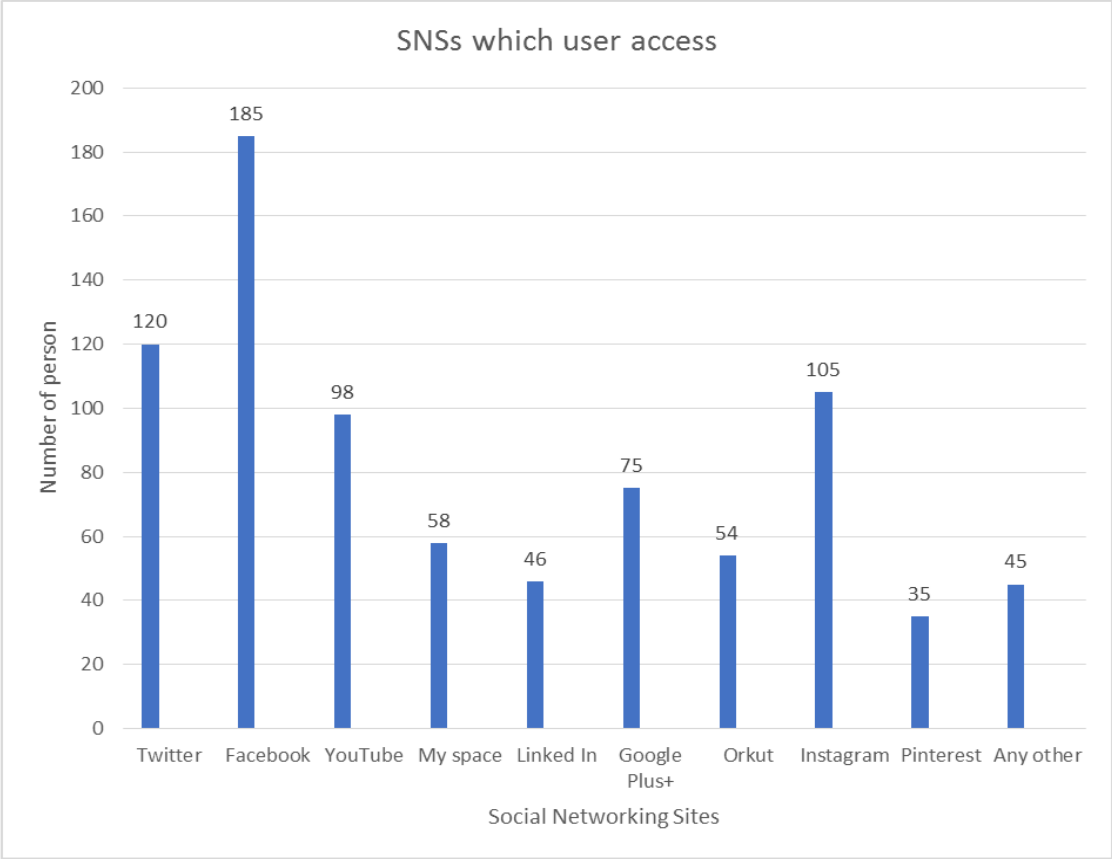



**Chart 8**

According to chart 8, every people use different kinds of social networking sites. According this chart, 185 people out of 200 people, response that they access Facebook daily, 120 people response that use twitter daily, 105 people use Instagram, 98 people accesses You Tube, 58 people accesses My space, 46 people Linked In, 75 people used Google Plus+, 35 people used Pinterest, 54 people used Orkut, and 45 people response that they accesses other social networking sites like WeChat, Skype, Viber, Snapchat, Telegram, etc. In the questionnaire next question is that, "For what purpose do you use Social networking sites?" Regards this question researcher prepare chart 9 on the basis of collected data.

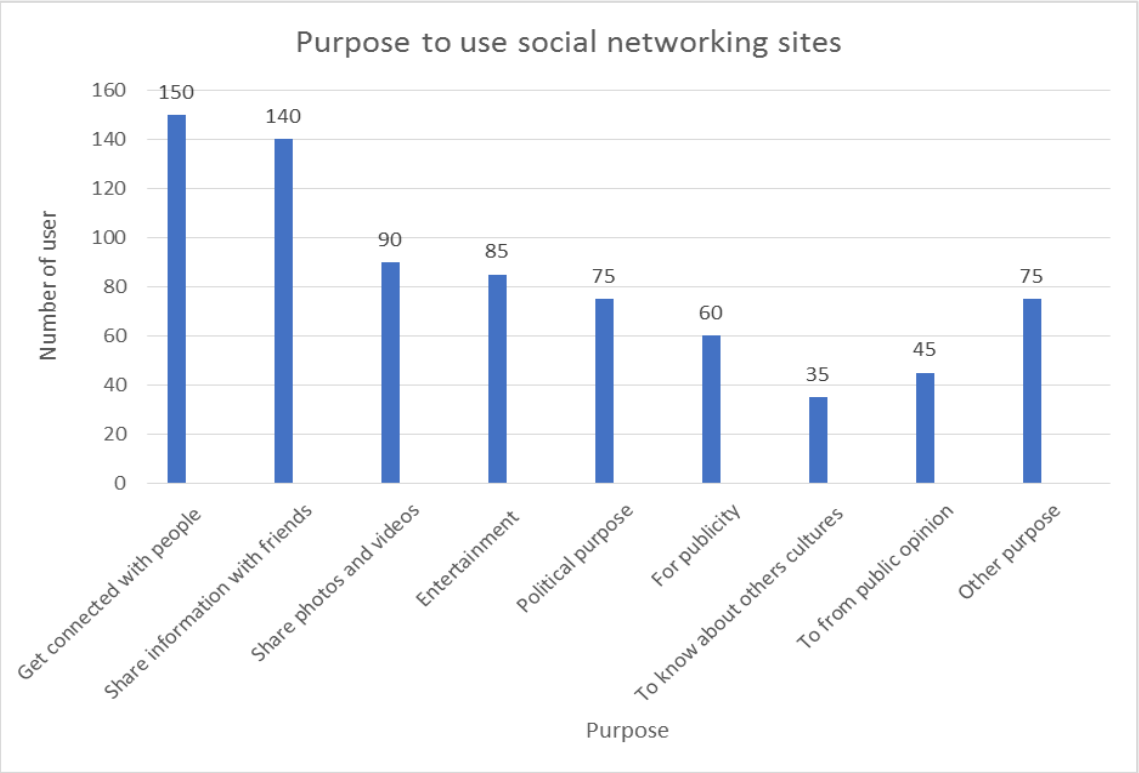



**Chart 9**

According to chart 9, 150 people out of 200 people use social networking sites for connect with other people by Facebook, Instagram etc. 140 people use social networking sites for share information with friends, and family. 90 people use SNSs for share photo and video to their family friends, college groups, etc.75 people use SNSs for political purpose like support the propaganda of the political party, support the parties by like the party moto, etc. 85 people use SNSs for entertainment. 60 people use SNSs for publicity. 35 people use SNSs to know about the others community culture. 45 people response that they are use SNSs for get the public opinion in any matter which is related to society or public welfare. 75 people response that they are use SNSs for more other purpose. In the questionnaire next question is that, "When you use social networking sites then do you read carefully data privacy policy?" Regard this question researcher prepare chart 10 on the basis of collected data.

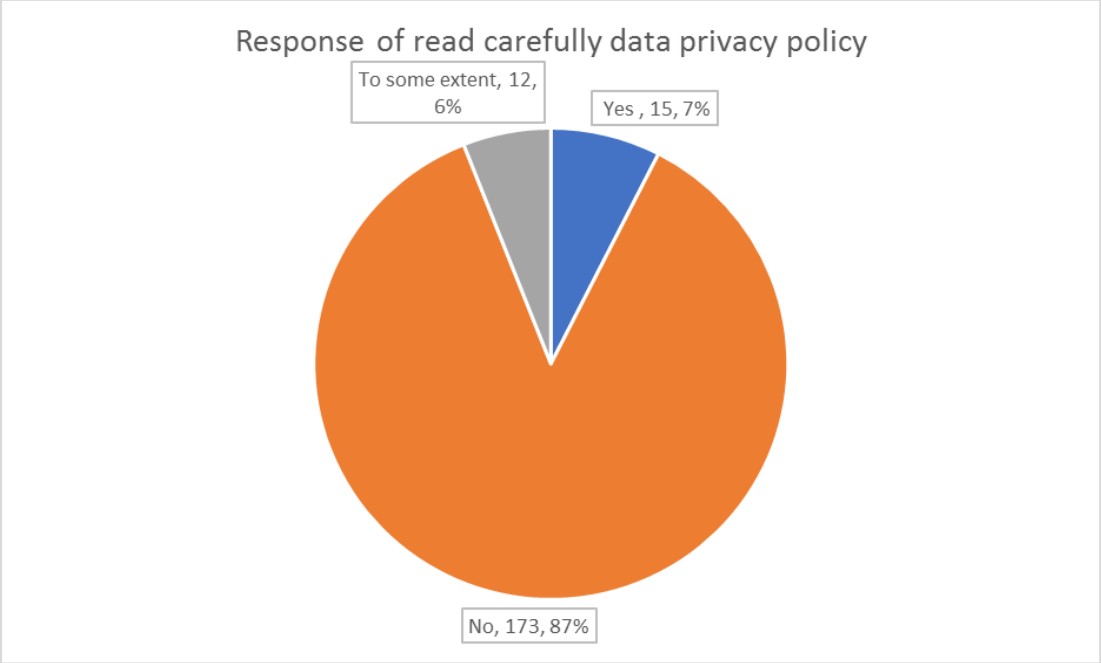



**Chart 10**

According to chart 10, 173 people out of 200 people response that they don't read the privacy policy carefully when they use social networking sites. It means 87 % people response that they use social networking sites daily but they cannot read the term and privacy policies of that social networking sites. They use different social networking sites (See in chart 8) for different purpose (See in chart 9) daily, but they cannot read the privacy policies. Due to that negligence breach data privacy of that user. 15 out of 200 response that they are read the privacy policy carefully. It means approximate 7 % people read privacy policy carefully. Its very fey amount that, user read privacy policy carefully. While 12 people response that they are read privacy policy to some extent. It means 6 % people read privacy policy but not wholly read. Due to this reason's user data privacy breach.

According to chart 4, chart 5, chart 6, chart 7, chart 8, chart 9, chart 10, researcher analysis that 95 % people have account on different social networking sites (see chart 4), like twitter, Instagram, Facebook, Orkut, Myspace, etc. (see chart 8). Approximate 85 % people use social networking sites daily (See chart 6). It means maximum person use social networking sites for their progressive life. They use social networking sites for information, send and receive mail, share photo and videos, for entertainment, etc (See chart 3). In that users, approximate 53 % people

use social networking sites (SNSs) more than 5 hours daily. 22 % people use SNSs 2-5 hours daily, while 12 % people use SNSs 1-2 hours daily and 13 % people use SNSs 0-1 hours daily. (See chart 7). But 87 % user don't read privacy policy when they are use social networking sites, only 7 % user read privacy policy carefully when they are use social networking sites. (See chart 10)

It means maximum number of persons use social networking sites daily but they are not read privacy policy carefully. It seems that they are not aware their data privacy. In the questionnaire next question is that, "Do you know about Privacy?"

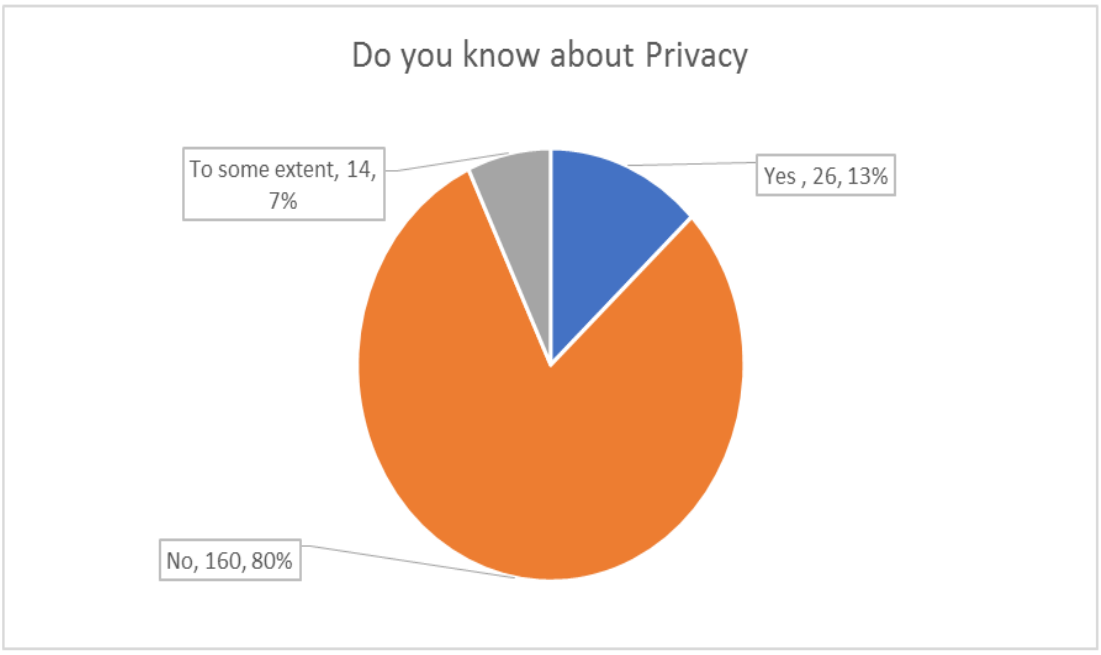



**Chart 11**

In this regard's researcher prepare chart 11 on the basis of collected data. According to chart 11, 160 people out of 200 response that they are not know about the Privacy. it means 80 % people have no any knowledge about Privacy. 26 people response that they are known about privacy. its means only 13 % people known about privacy, while 7 % people response that they have known about the privacy to some extent. It means maximum user have no knowledge about privacy. In the questionnaire next question is that, "Do you know, in the case of **Justice K. S. Puttaswamy (Ret.) and others Vs. Union of India and others,** Supreme court of India held that "Right to Privacy" is a fundamental right?" In this regard's researcher prepare chart 12 on the basis of collected data.

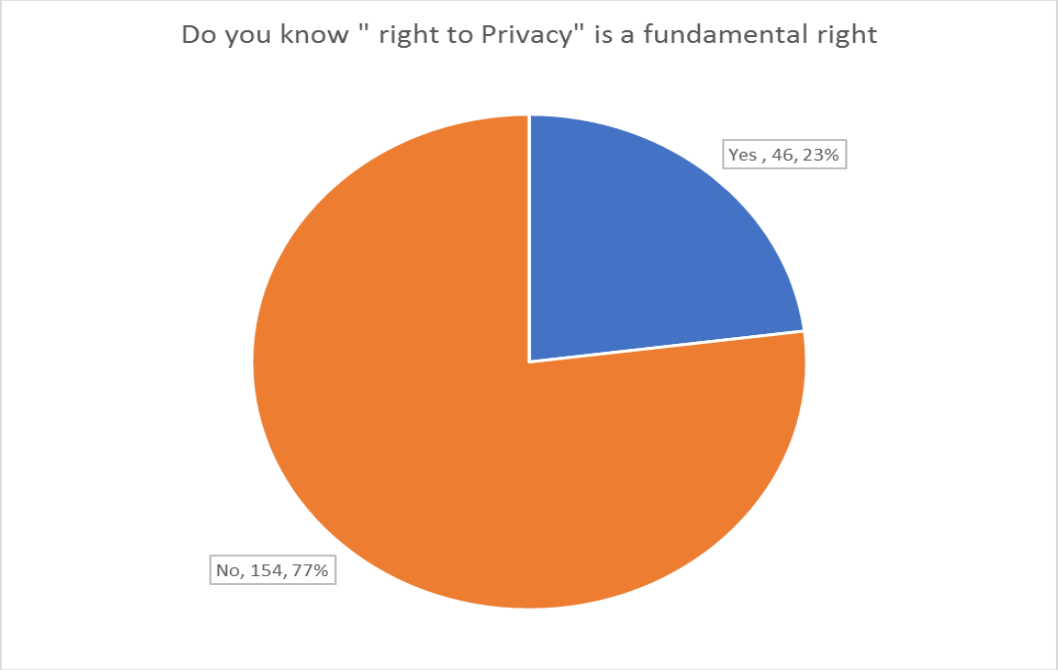



**Chart 12**

According to chart 12, 154 people out of 200 response that they do not know that "right to privacy" is a fundamental right. It means approximate 77 % user have no knowledge that right to privacy is become fundamental rights in the case of **Justice K. S. Puttaswamy (Ret.) and others Vs. Union of India and others.** While 23 % user have knowledge that right to privacy is become fundamental rights. It means maximum user unaware their privacy. In the questionnaire next question is that, "Do you know about Data Privacy?" In this regards researcher prepared chart 13 on the basis of collected data.

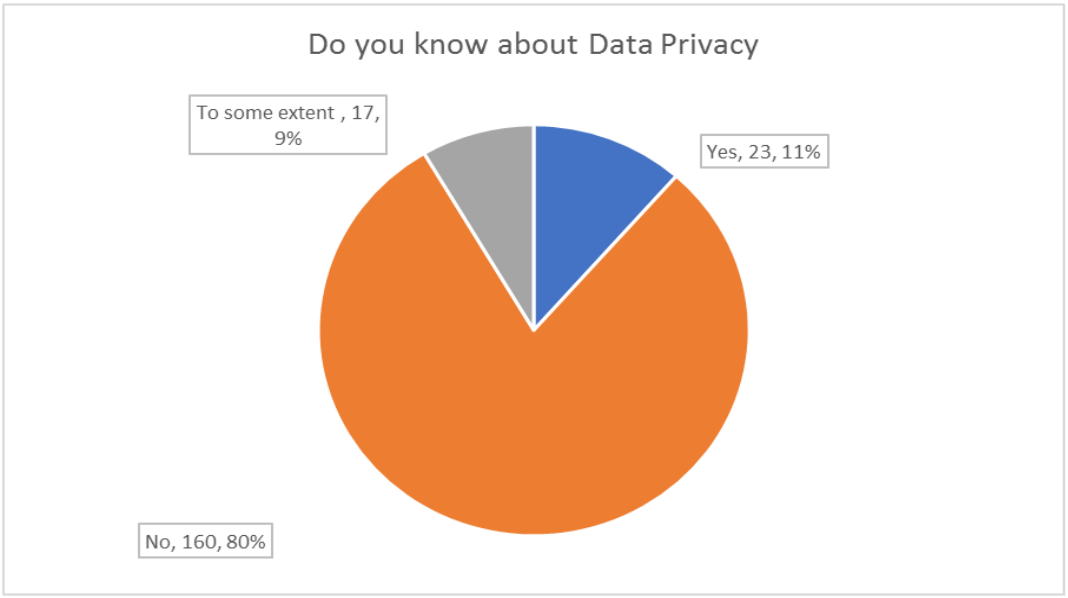



**Chart 13**

According to chart 13, 160 people out of 200 response that they do not know "what is Data Privacy?". They have no any idea about Data Privacy. it means approximate 80 % user do not know about data privacy. it means they do not know "what is Data Privacy?", How Data privacy Breach? what remedies available for the breach of Data Privacy? etc. According to chart 13, 23 people out of 200 people response that they know about "Data Privacy". it means approximate 11 % use know about data privacy. while 17 people out of 200 people response that they know about data privacy to some extent. It means 9 % user have some extent knowledge about the data privacy.

In the questionnaire next question is that, "Do you assume that Indian Judiciary plays a vital role for the protection of data privacy?" In this regard chart 14 prepared by the researcher on the basis of the collected data.

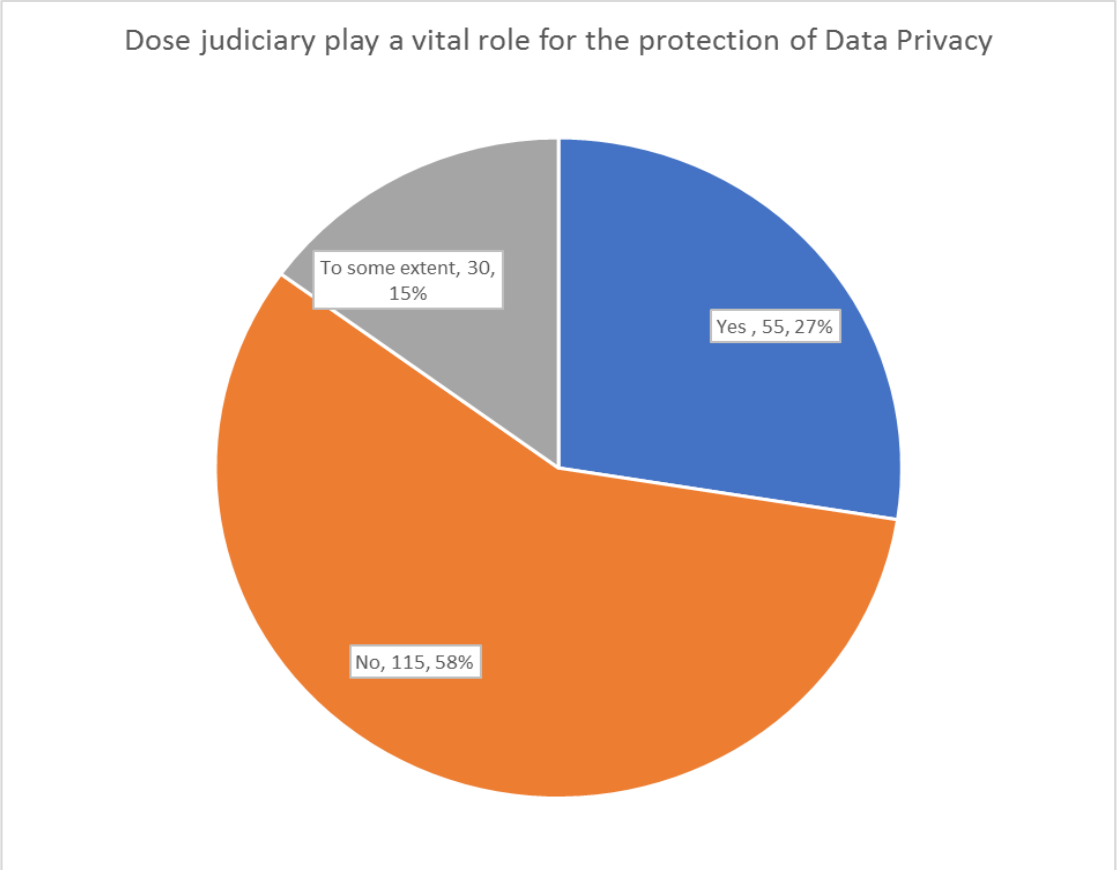



**Chart 14**

According to chart 14, 115 people out of 200 people response that they don't assume that the Indian judiciary plays a vital role for the protection of data privacy. it means approximate 58 % people not assume that the Indian judiciary plays a vital role for the protection of data privacy, because in India there are no any specific Act related to Data Privacy.

While 55 people out of 200 people response that Indian judiciary play a vital role for the protection of data privacy. it means 27 % user assume that Indian judiciary play a vital role for the protection of data privacy. 30 people out of 200, it means approximate 15 % people response that Indian judiciary to some extent play a vital role for the for the protection of data privacy.

After the analysis of the chart 11, chart 12, chart13 and chart 14, Its cleared that, approximate 85 % people use social networking sites daily. It means maximum person use social networking sites for their progressive life. They use social networking sites for information, send and receive mail, share photo and videos, for entertainment, etc (See chart 6). But they don't know about the data privacy. approximate 80 % people have no any knowledge about Privacy (see chart 11). They do not know about Data Privacy (See chart 13) and approximate 77 % user have no knowledge that right to privacy is become fundamental rights. Its show that the lack of awareness related to data privacy and their protections. So, its required that firstly aware the data user related their data privacy.

In the questionnaire next question is that, "Do you know about 'Sensitive personal Data'?" Regards this question researcher prepared chart 15 on the basis of collected data.

In chart 15, it is show that how much user know about "Sensitive Personal Data" and how much user don't know about Sensitive personal data, and how much user know about Sensitive Personal Data to some extent.

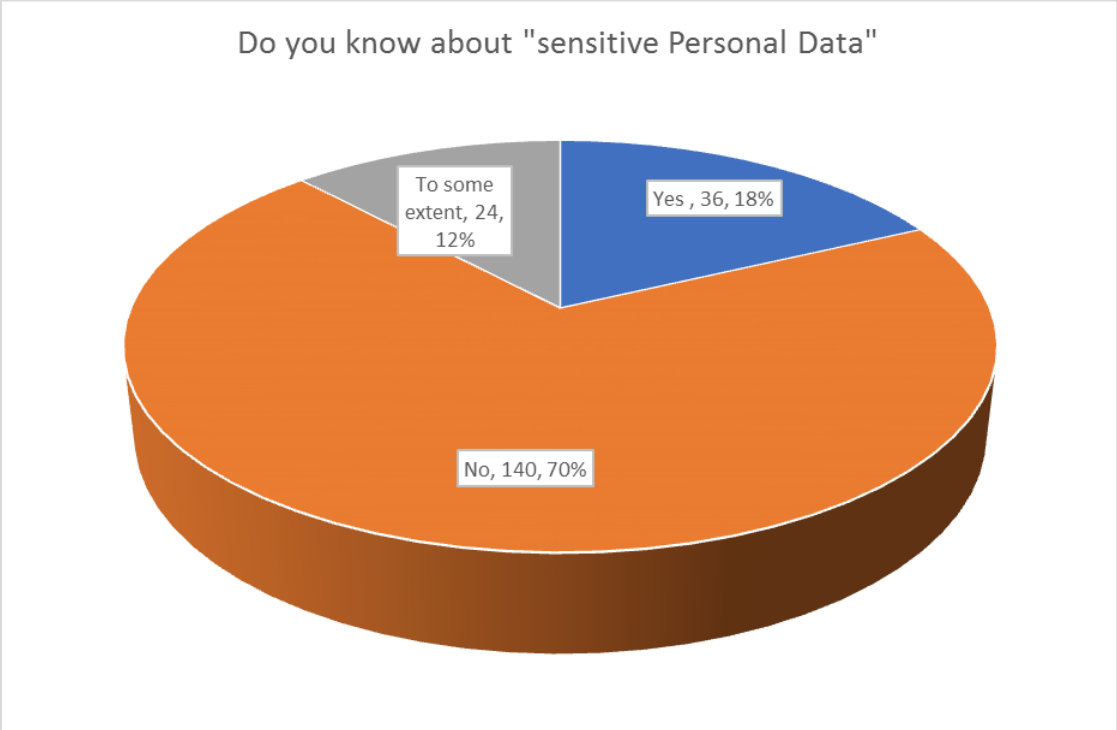



**Chart 15**

According to chart 15 it is cleared that, 140 users out of 200 user response that, they don't know about Sensitive Personal Data. It means approximate 70 % user of internet they do not have any idea of "Sensitive personal Data". They don't know. E-mail id, password, Bio- matric, Aadhaar Number, Finger- prints, ATM Pin, GPS Locations, etc are Sensitive Personal Data.

24 use out of 200 user response that they are known about Sensitive Personal Data to some Extent. It means 12 % user know about the Sensitive Personal Data to some extent. While 36 users out of 200 use response that they are know about the Sensitive Personal data. It means only 18 % user know about sensitive personal data. This is big problem for data Privacy.

In the questionnaire next question is that, "Do you share your Aadhaar Number to any social welfare scheme/ Bank/ Fill-up examinations form, etc.?" Regards this question, researcher prepared chart 16 on the basis of collected data.

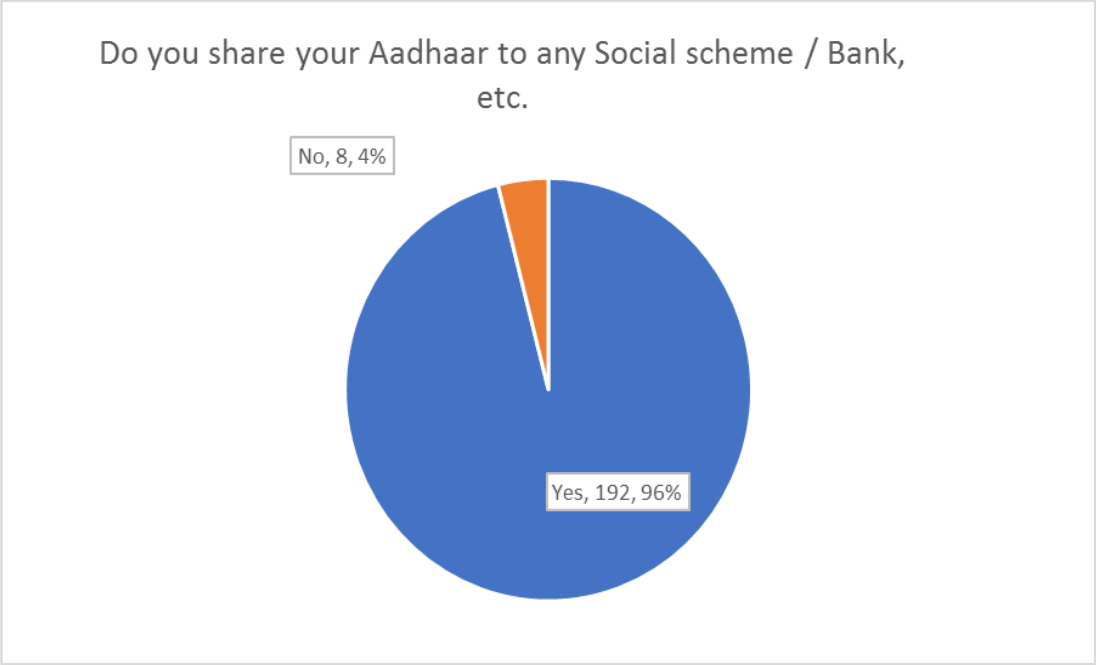



**Chart 16**

According to chart 16, 192 people out of 200 people response that they are share their Aadhaar number to different social welfare scheme / Bank / Fill-up different Examinations form etc. while 8 people out of 200 people response that they are not share their Aadhaar number to any social welfare scheme/ bank. Different examination forms. It means approximate 96 % people share their Aadhaar Number for Social welfare scheme/ Bank etc.it means maximum number of people share their Aadhaar Number for different purpose.

In the questionnaire nest question is that, “Do you assume that your personal data and Aadhaar Number which is share to any social welfare scheme/ Bank/ fill-up examinations form, etc are safe?” Regards this question, researcher prepare chart 17 on the basis of collected data.

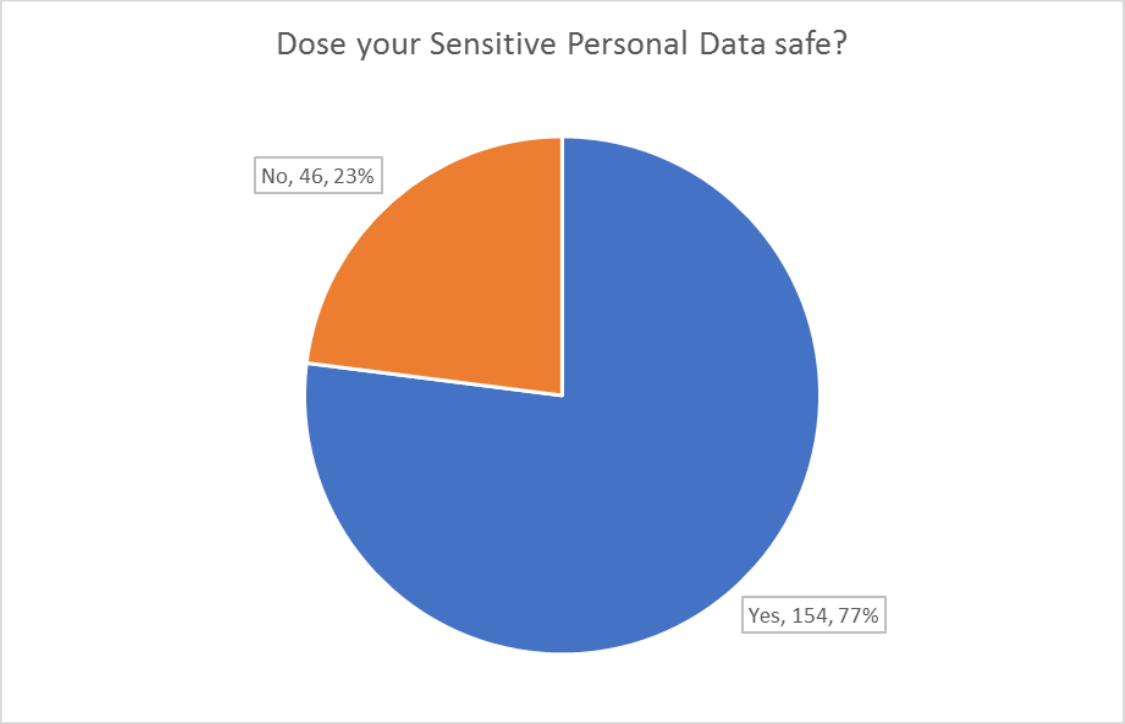



**Chart 17**

According to chart 17, it is cleared that, 154 people out of 200 people response that they don't assume that their personal data and Aadhaar number which is share to different social welfare scheme or Bank or fill-up examinations form, are safe. It means approximate 77 % people assume that their personal data and Aadhaar number are not safe which are share to governmental and non-governmental scheme, Bank, different SNSs, etc.

46 people out of 200 people response that they assume that their personal data and Aadhaar number are safe which is share to different social welfare scheme/ Bank, etc.

It means approximate 23 % people assume that their Personal data and Aadhaar number are safe. In the questionnaire next question is that, "Do you know about your rights related to Data Privacy?" Regards this question researcher prepared chat 18 on the basis of the collected data.

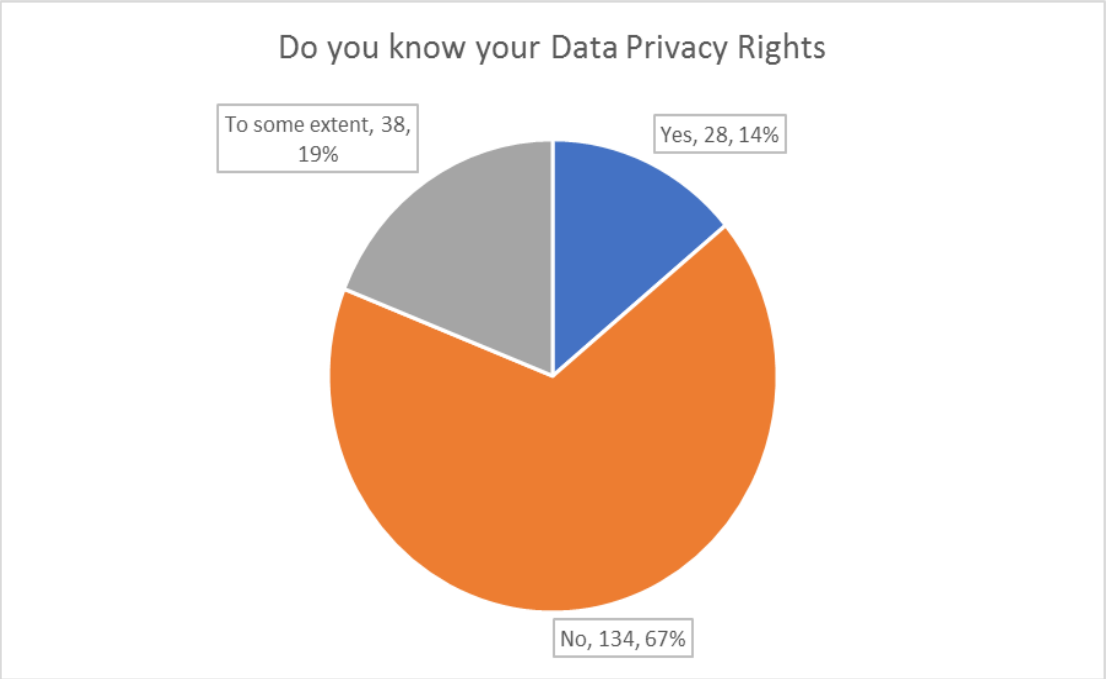



**Chart 18**

According to chart 18, it is cleared that, 134 people out of 200 people response that they don't know about their rights related to Data Privacy. it means approximate 67 % people have no knowledge about their rights related to Data privacy. they are unaware their data privacy rights. While 28 people out of 200 people response that they are known about their Data Privacy rights. It means approximate 14 % people are aware their data privacy rights. In this chart, 38 people out of 200 people response that they have some extent to knowledge about their Data Privacy Rights. It means approximate 19 % people have some extent of knowledge about their Data Privacy Rights.

According to chart 15, chart 16, chart 17, and chart 18, researcher analysis that, Approximate 96 % people share their Aadhaar Number for Social welfare scheme/ Bank etc.it means maximum number of people share their Aadhaar Number for different purpose. (See chart 16). But approximate 70 % user, they don't have any idea of "Sensitive personal Data". They do not know. E-mail id, password, Bio-matric, Aadhaar Number, Finger- prints, ATM Pin, GPS Locations, etc are Sensitive Personal Data. They have no any idea that Aadhaar Number, personal data, E-mail Id, Bank Passbook, PAN Number, etc. are sensitive personal data (See chart 15). Approximate 77 % people assume that their personal data and Aadhaar number are

not safe, which are share to governmental and non-governmental scheme, Bank, different SNSs, etc. (See chart 17).

So, its required that aware to the people related to their "Sensitive Personal Data" and "Rights related to Data Privacy" In the questionnaire next question is that, Do you know about "The Personal Data Protection Bill, 2018?" Regards this question researcher prepare the chart 19 on the basis of collected data.

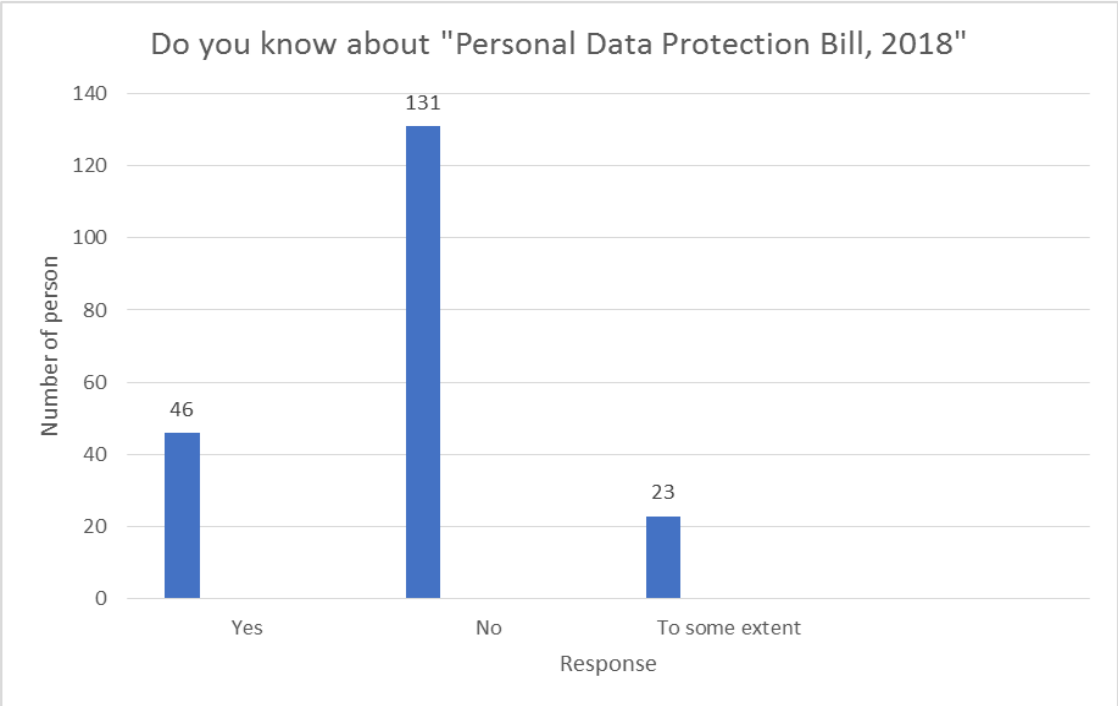



**Chart 19**

According to chart 19 it is cleared that, 131 people, out of 200 people response that they do not know about "The Personal Data Protection Bill, 2018". It means 65 % people don't know about the, Personal data, Sensitive Personal Data, Data User, Data Fiduciary, Genetic Data, Data Authorities, Rights of Data users, Seven key Principles of Data Privacy, Breach of data privacy and their compensations, etc. it means maximum number of person do not know about this Bill.

In this chart 46 people, out of 200 people response that they are known about the "Personal Data Protection Bill, 2018". It means approximate only 23 % people well know about this Bill. While 23 people, out of 200 people response that they

know about the Personal Data Protection Bill to some extent. It means approximate 12 % people response that they know this bill but some extent.

In the questionnaire next question is that, "Do you know about the "General Data Protection Regulation (GDPR)?" Regard this questions researcher prepare chart 20 on the basis of collected data.

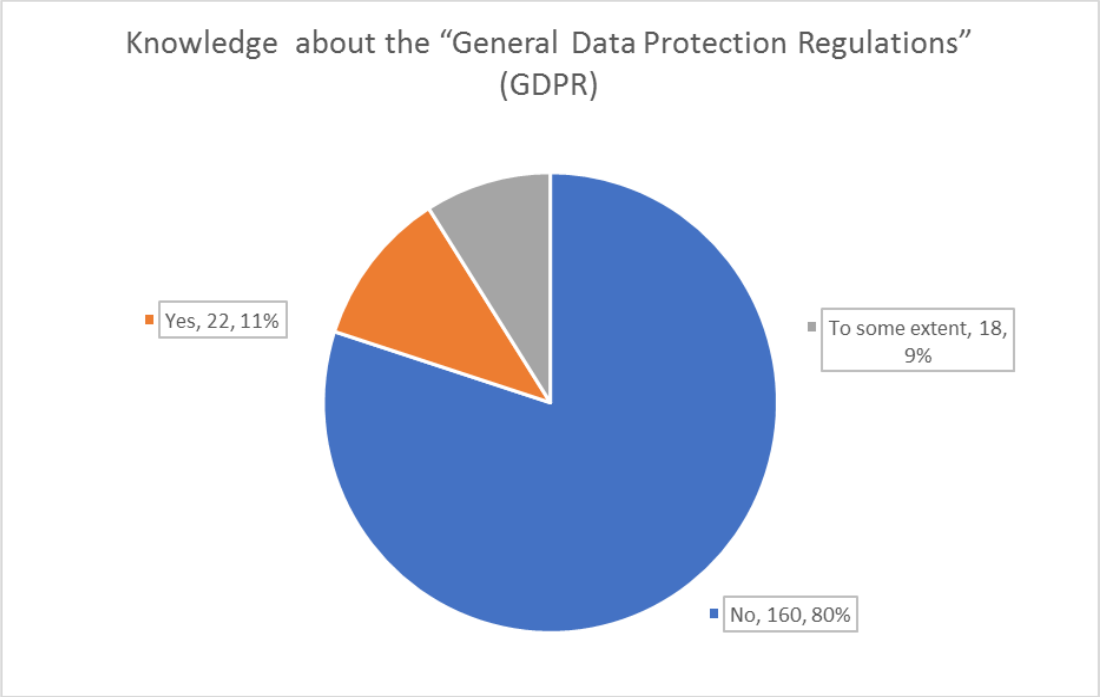



**Chart 20**

According to chart 20, it's clear that, 160 people, out of 200 people response that, they don't know about the "General Data Protection Regulation (GDPR). It means approximate 80 % people have no any kind of knowledge about the GDPR. They do not know that's GDPR is a legal instrument related to the Data Protection at the International level.

In this chart, 22 people, out of 200 people response that they are known about the GDPR. It means only 11 % people know about the GDPR. While 12 people out of 200 people it means only 6 % people response that they know about the GDPR to some extent. In the questionnaire next question is that, "Do you know, where would you go for remedies, in case of breach of data privacy?"

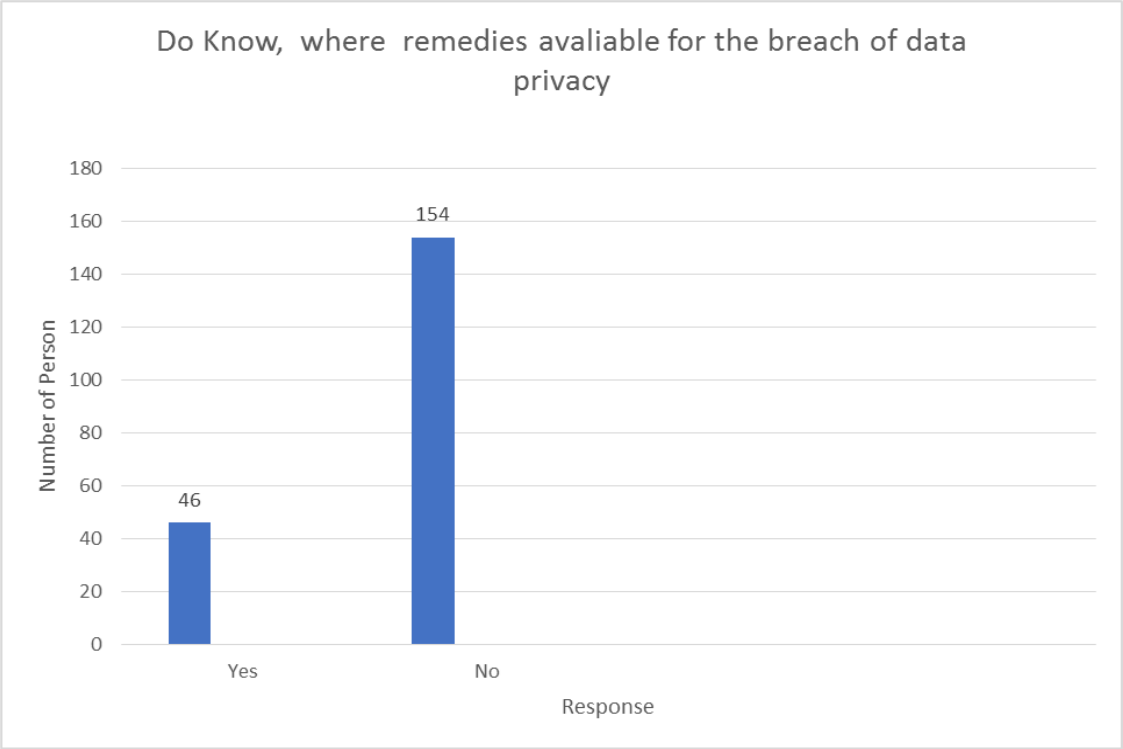



**Chart 21**

According to chart 21 its cleared that, 154 people out of 200 people response that they have no any knowledge that if breach their data privacy, where they go for remedies. It means approximate 77 % people don't know, if their data privacy breach then where they go for remedies. While 46 people out of 200 people response that they are know that where remedies available when breach their Data Privacy. it means only 23 % people know that where remedies available after the breach of Data Privacy. maximum number of people have no any idea where remedies available for the breach of data privacy.

In questionnaire last question is that, Do you know "what are remedies available when any one breach your data privacy?" Regards this question researcher prepare chart 22 on the basis of collected data.

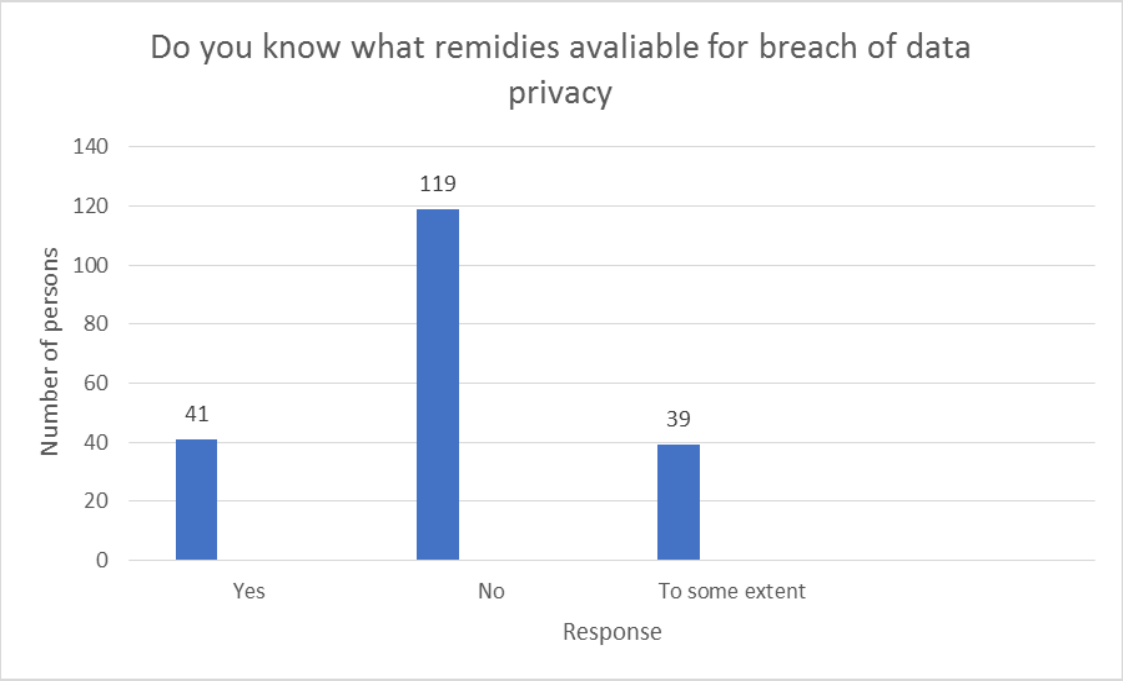



**Chart 22**

According to chart 22 its cleared that, 119 people out of 200 people response that, they don't know what remedies available for the breach of data privacy. it means approximate 59 % people have no any idea that what remedies available for the breach of data privacy. In this chart 41 people out of 200 people, it means approximate 21 % people response that they are know what remedies available when breach their data privacy. while 39 people out of 200 people, it means 20 % people response that they are known to some extent, what remedies available for the breach of their data privacy.

### 6.2. Analysis of collected Data

In India maximum persons have mobile, laptop, tablet etc. Every person has Aadhar Number, E- mail Id, Facebook Id., PAN number, etc. they use these in their life, but they do not know these are their Personal Data. They share their personal data, Sensitive personal data, etc when the use internet or to get profit of any social welfare scheme. Or fill-up their examination form, or open Bank accounts, etc. They not aware about breach of their data privacy. They have no any idea, what remedies available? and where these remedies are available?

This regards researcher prepared different kinds of 22 charts, on the basis of collected data. According to these chart researcher analyses that,

Approximate 98% people use internet in their daily life. It is the need for our daily life. Our maximum activity related to our progressive life is drive by the internet. Its play a vital role in our daily life.( See chart 1) They are use internet for information, send and receive E-mails, for social networking sites, for Professional issue, use for gaming, for instant messaging, for sharing photos and videos, for social media, for educational purpose, for online shopping, for entertain, for download music, etc.( See chart 3). This regards approximate 95 % internet user have account on social networking sites. (See chart 4). But approximate 75% people have knowledge that how to use internet, while, 15% have no knowledge that how to use internet, and 10% people have some extent knowledge that how to use internet. (See chart 2). They use internet for various purpose but they do not know about how to use internet and How protect our data privacy?

Approximate 85 % people use social networking sites daily. It means maximum person use social networking sites for their progressive life. They use social networking sites for information, send and receive mail, share photo and videos, for entertainment, etc. while approximate 8 % people use social networking sites Bi-weekly, 4 % people use social networking sites weekly, and 3 % people use social networking sites occasionally. (See chart6)

Maximum person uses Social networking site for their progressive life. They spend time on social networking sites on maximum time. Approximate 53 % people use social networking sites (SNSs) more than 5 hours daily. 22 % people use SNSs 2-5 hours daily, while 12 % people use SNSs 1-2 hours daily and 13 % people use SNSs 0-1 hours daily. (See chart 7) It means maximum people spend much time on social networking sites but they not aware about their data privacy.

When they use SNSs then they do not read privacy policy carefully. According to chart 10, its cleared that, 87 % user cannot read privacy policy when they are use social networking sites, only 7 % user read privacy policy carefully when they are use social networking sites. (See chart 10). It means maximum number of persons use social networking sites daily but they are not read privacy policy

carefully. It seems that they are not aware their data privacy. They have no knowledge about their data privacy.

According to chart 11 its cleared that, Approximate 80 % people have no any knowledge about Privacy, while, only 13 % people known about privacy and 7 % people have knowledge about the privacy to some extent. It means maximum user have no knowledge about privacy.

And according to chart 12, approximate 77 % user have no knowledge that right to privacy is become fundamental rights in the case of **Justice K. S. Puttaswamy (Ret.) and others Vs. Union of India and others.** While 23 % user have knowledge that right to privacy is become fundamental rights. It means maximum user unaware their privacy. They do not know that Right to privacy held that a fundamental right in the Constitution of India.

According to chart 14, maximum number of people not believe that Indian Judiciary play a vital role for the protection of data privacy. Approximate 58 % people not assume that the Indian judiciary plays a vital role for the protection of data privacy, because in India there are no any specific Law related to Data Privacy.

What is Data Privacy? maximum number of people answered that they do not know about the data privacy. According to chart 13, approximate 80 % user do not know about data privacy. it means they do not know "what is Data Privacy?", How Data privacy Breach? what remedies available for the breach of Data Privacy? etc. It is also cleared that; approximate 67 % people have no knowledge about their rights related to Data privacy. They are unaware their data privacy rights. Only approximate 14 % people are aware their data privacy rights. While, approximate 19 % people have some extent of knowledge about their Data Privacy Rights. This means large number of people use SNSs but the not know about the data privacy rights. Due to lack of awareness this problem is arise.

In India maximum number of people have no any idea related to "Sensitive Personal Data". They do not know about "Sensitive Personal Data". They do not know that, Passwords, Financial data, Health data, Official identifiers which would include government issued identity cards, Sex life and sexual orientation, Biometric and genetic data, Transgender status or intersex status, Caste or tribe, Religious or

political beliefs or affiliations, these are the Sensitive Personal Data. The do not aware their Sensitive Personal Data. In Chart 15, it is cleared that, approximate 70 % user of internet they do not have any idea of "Sensitive personal Data". They do not know. E-mail id, password, Bio- matric, Aadhaar Number, Finger- prints, ATM Pin, GPS Locations, etc are Sensitive Personal Data. 12 % user know about the Sensitive Personal Data to some extent. While only 18 % user know about sensitive personal data. This is big problem for protection of data Privacy.

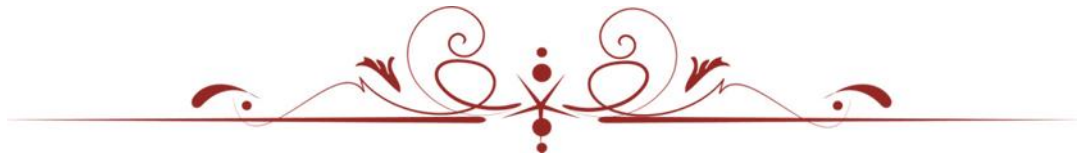
It is cleared that maximum number of persons have no knowledge about the Sensitive Personal Data. But they share their Sensitive Personal data like Aadhaar Number, Biometric Data, Finger prints, etc. to any social welfare scheme, Bank Account, fill- up examination forms etc. Chart 16 cleared that; approximate 96 % people share their Aadhaar Number for Social welfare scheme/ Bank etc. it means maximum number of people share their Aadhaar Number for different purpose. They share their Aadhaar number, sensitive personal data etc but they assume that, their Sensitive personal Data are not safe. Chart 17, cleared that, approximate 77 % people assume that their personal data and Aadhaar number are not safe which are share to governmental and non-governmental scheme, Bank, different SNSs, etc. while, approximate 23 % people assume that their Personal data and Aadhaar number are safe. It means a large number of people assume that they share their sensitive personal data to governmental and non -governmental agency are not safe.

In the "Personal Data Protection Bill, 2018" provide provisions related to Data Privacy. In this Bill, define the Data Personal Data, Sensitive Personal Data, Biometric Data, Genetic Data, Data Principal, Data Processer, Anonymized Data, etc. in this Bill provide provisions related to Rights of Data Principal, Duty and obligations on Data Processor, what and where remedies available for breach of data Privacy. But approximate 65 % people don't know about the, Personal data, Sensitive Personal Data, Data User, Data Fiduciary, Genetic Data, Data Authorities, Rights of Data users, Seven key Principles of Data Privacy, Breach of data privacy and their compensations, etc. it means maximum number of person do not know about this Bill. approximate 77 % people don't know, if their data privacy breach then where they go for remedies and what remedies available for the breach of data privacy.

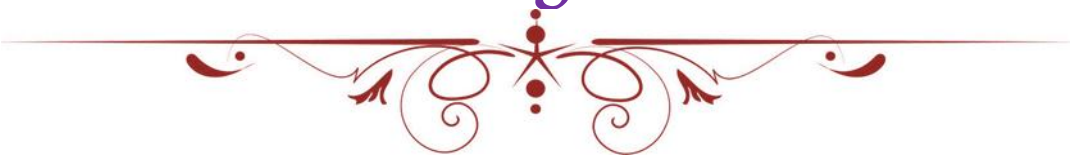
## 6.3. Conclusion

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 Remark



# Chapter VII
# Concluding Remark

## 7.1. Conclusions

*"Privacy is a common value in that all individuals value some degree of privacy and have some common perceptions about privacy. Privacy is also a public value in that it has value not just to the individual as an individual or to all individuals in common but also to the democratic political system …"*[1]

Right to Privacy is a valuable human right for every individual. It is a variable concept and varies with the passage of time, place and society. Therefore, it is not easy to define 'Privacy' in strict sense of the term. Privacy generally means, the right to be let alone (Justice Cooley, 1888). In 1890, Louis Brandeis and Samuel Warren published a seminal article in the Harvard Law Review, titled "The Right to Privacy," where it was observed that, the object of Privacy is to protect 'inviolate personality.' Next important landmark in the field of Privacy, is the book written by Prof. Alan F. Westin, titled "Privacy and Freedom," 1970. It defines Privacy as the desire of individuals for solitude, intimacy, anonymity and reserve. According to him, Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent, information about them is communicated to others.

Therefore, Right to Privacy cannot be described as a single human right, rather it is a bundle of rights and it includes human being's choice over his or her own personal affairs to decide the extent of public disclosure of the same. In brief, Privacy means, freedom from unauthorized and unwarranted intrusion into one's private and personal life. In the modern age, various new dimensions of Right to Privacy have been emerged, like Privacy of Family, Home and Correspondence, Privacy of Marriage, Privacy of Information, Workplace Privacy, Privacy of Celebrity Life, Health Care Privacy and so on.

In the present digital age, good governance is impossible without the proper implementation of digital services and the active support of citizens. However, at the

[1] Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, 1995, pp.213, 225.

same time, governments need to make sure that citizens are protected from any type of harm while using different digital services and uphold the human rights framework. A common digital platform can gather different sets of data that help to coordinate the governance work properly, smoothly, quickly, and effectively. The potential of having a common digital platform for governance cannot be underestimated, especially in developing countries where mobile networks are growing very rapidly. Thus, digital empowerment is increasingly seen as the new paradigm of good governance.

For good governance 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.

The Council of Europe was one of the first international bodies to begin developing normative response to the threats posed by computer technology to privacy related interest. It is the only international body to have draft a multilateral treaty dealing directly with data privacy. It was the legally binding international instrument in the data protection field.

In January 1981 the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention entered into force in October 1985. It is important to recognize that the

Convention is a multilateral treaty as distinct from a statutory act of the Council of Europe. It is therefore legally binding under international law only upon those states that express consent to be bound through the formal act of ratification or accession. This Convention is also open to accession by non-member states of the Council of Europe but so far it has not attracted any non-member parties. The Convention was the first binding international instrument to protect individuals against abuses in the collection and processing of their personal data. It covers automated personal data files and automatic processing of personal data in the public and private sectors.

In this convention main purpose of the convention is to "to introduce basic principles for fair information processing" and "to establish rules and restrictions on transborder data flows". This convention provide provision for processing of data and principles related to data privacy and data protections. The heat of the Convention lies in Chapter II which is broad-brush fashion, setout basic principal for Processing of personal data. Article 4 begins with an obligation on state parties to "take the necessary measures" to give effect to the basic principles for data protection in domestic law.

The Directive also imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to and processed in countries outside Europe. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. More than forty countries now have data protection or information privacy laws. More are in the process of being enacted.

The evidence gathered during this study showed clearly that the success or failure of privacy and data protection is not governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work. The stronger, results oriented approach aims to protect data subjects against personal harm resulting from the unlawful processing of any data, rather than making personal data the building block of data protection regulations. It would move away from a regulatory framework that measures the adequacy of data processing by measuring compliance with certain formalities, towards a framework that instead requires certain fundamental principles

to be respected, and has the ability, legal authority and conviction to impose harsh sanctions when these principles are violated.

Data protection is an issue that is gaining increasing importance as our transnational exchange of private information grows. While the E. U. has adopted stringent legislation to protect data, and the U.S. has reached agreement with the E.U. to offer protection, the Indian laws remain unsatisfactory. It is anticipated that India will soon enact legislation which will provide acceptable protection to private data.

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***. 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 ***R. M. Malkani vs State of Maharashtra*** case, 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.

In ***X. Vs. Hospital Z***, The Supreme Court was confronted with the test of striking a balance between two conflicting fundamental rights: the Aids patients right to life which included his right to privacy and confidentiality of his medical condition, and the right of the lady to whom he was engaged to lead to healthy life. Supreme Court held that right to privacy is an essential component of right to life but it is not absolute and may be restricted for the prevention of crime, disorder or protection of health or morals or for the purpose of protection of rights and freedom of others.

The most significant development in respect of protection of privacy is the recent decision of the High Court of Delhi in the **Naz Foundation Case**, in which the Court held that Section 377 of the Indian penal code violated Articles 21, 14 and 15 of the Constitution, insofar as it criminalizes consensual sexual acts of adults in private. Because of the doctrine of severability, it 'will continue to govern non-consensual penile non-vaginal sex and penile nonvaginal sex involving minors. Right to privacy in respect of abortion is another such area which has not discussed in any Indian legislation.

Recently in ***Suchitra Srivastava and others v. Chandigarh Administration*** the Supreme Court observed that, there is no doubt that a woman's right to make reproductive choices is also a dimension of personal liberty as understood under Article 21 of the Constitution of India. It is important to recognize that reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a women's right to privacy, dignity and bodily integrity should be respected.

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.

Present time we are living in Digital Era. Where everything is digital. Such as by e-library we do research on different fields, study books, magazine, articles, make their presentations, etc. by e-mail people send and received instant massage and information. By e-shopping people ordered daily use items, fashions items books, cloths etc. and received that items at their door step. By e-ticket people book their train ticket, Airplane ticket, movies ticket, museum and park ticket, etc. By e-payment people payment through Net Banking or mobile banking apps, when they purchase anything in anywhere. People use internet for travels and food orders, such as Ola, Uber, Swigi, Zomato, etc and share their personal data to the company. People use social media sites for Communications such as Facebook, Twitter. You Tube use for see and download video, and as well as uploads data in the internet. Internet has stored a massive amount of data or information and it is nothing but the Big Data.

Dynamic nature of social media data is a significant challenge for continuously and speedily evolving social media sites.

When we use these SNSs and Social Media then we share a lot of personal data and sensitive personal data to that sites. These SNSs are store our data and share our data to others Social networking sites withought the consent of the data Principal. due to this reason Social networking sites are breach our data privacy. So, its required that Government draft a specific legislation for the protections of data privacy. Maximum people don't know about data privacy so its required that aware people to their data privacy.

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.

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, State Bank of India Act, 1955 Credit Information Companies (Regulation) Act, 2005 , Credit Information Companies Regulations, 2006, The Mental Health Act, 1987, Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017

Aadhaar (Data Security) Regulations, 2016 Indian Telegraph Act, 1885, Telecom Regulatory Authority of India act, 1997, Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act-2016 etc.

The Credit Information Companies (Regulation) Act 2005, although it is not yet fully operational, includes privacy principles which cover most usual data protection rights, though only in relation to the context of credit reporting. There is otherwise as yet no significant legislation protecting personal information in India, though some provisions in the ITAA2008 may emerge as significant depending on regulations made and implementation, particularly concerning data security. There is no special protection for personal information imported into India from other jurisdictions.

There is an effective right of access to personal information in the public sector, under the Right to Information Act 2005, and this right of access is probably the most significant aspect of data protection in India at present. There is also protection within India against telemarketing through the Telecom Unsolicited Commercial Communications Regulations 2007. Significant though these areas are, it cannot be said that privacy principles apply to most aspects of Indian life.

The Credit Information Companies (Regulation) Act 2005, although it does include a full set of privacy principles, is lacking in comprehensive enforcement measures. It relies almost entirely on prosecution of offences, either through the courts or administratively by the Reserve Bank. There is no obvious way for complaints to be made. The Reserve Bank has extensive directive powers, but is not a consumer protection agency and its interests are more obviously in creating a modem credit economy than in protecting consumer privacy. However, the system is untested, and it is necessary to wait and see.

There is as yet no significant self-regulation for the purposes of privacy protection in India. There are no aspects of India's data protection which would unequivocally be regarded as 'adequate' by European Union standards as yet, though further investigation might indicate that there are some sectoral areas of adequacy. This could also change as rules are made under existing legislation. The most likely candidates (in decreasing order of likelihood) might be: The credit reporting system, but only after it has been tested in practice; The right of access (but only in relation to

public authorities); The implementation of the security principle via both compensatory provisions (subject to how Section 43A is implemented) and offences; The provisions concerning opting out from direct marketing.

India is still at a very early stage of developing personal data protection, though some of the signs are promising. Balanced against this must be the increases in surveillance powers.

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. Companies cannot get full protection of data through that which ultimately forced them to enter into separate private contracts to keep their data secured. These contracts have the same enforceability as the general contract.

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. Going by the definition of personal data laid down by the European Union's data protection guidelines, "information concerning an identified and identifiable natural person" covers the scope of personal data. Therefore, if we follow this definition, the personal information provided by individuals during biometrics would be included.

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. The bill has been drafted wholly on the structure of the UK Data Protection Act whereas today's requirement is of a comprehensive Act. Thus, it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favorable to the today' requirement.

Fundamental right and after its analysis, it is justified to treat right to data privacy as an important right. From others interference and Infringement of individual liberty can only be satisfied the entire legal requirement as a right of data protection. 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,

To conclude the right to Data Privacy in India as in any other jurisdiction, though not statutory codified as yet. Its scope is by the lack of such a codification neither extremely narrow nor considerably wide. This implies that this aspect should be handled with a great deal of care and circumspection.

### 7.2. Suggestion

However, it is important to keep in mind that some real challenges exist and some new challenges are being added to those existing challenges. Governments, some security agencies, terrorist groups, private companies and other unnamed groups are scrutinizing the online world continuously. Thus, the issue of personal privacy, safety, and security must be taken care of properly.

So, an exceptional attention with innovative approach should be taken at the time of developing new digital platforms for public services, as users look for guaranteed quality, anonymity, privacy, and security. It is suggested to use Privacy Enhancing Technologies during the development process of those platforms. This is the time for a new deal on data, and governments need to ensure protection of personal data privacy.

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. Going by the definition of personal data laid down by the European Union's data protection guidelines, "information concerning an identified and identifiable natural person" covers the scope of personal data. Therefore, if we follow this definition, the personal information provided by individuals during biometrics would be included. 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.

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)** Privacy is not a well-defined right in U.S.A., U.K. and India. Therefore, at first it should be properly introduced as a well-defined right in the three countries removing all the vagueness, because without defining a right in concrete sense, its protection cannot be possible in full-fledged manner.

**2)** Express Constitutional protection of Right to Privacy and Data Privacy Protections is unavailable in U.S.A., U.K. and India, which is an impediment for its enforcement. Therefore, both U.S.A. and India should incorporate Right to Privacy and Data Privacy as a Fundamental Right under their Constitutions.

**3)** 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.

**4)** 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.

**5)** Both U.S.A. and U.K. have highlighted the areas of Data Privacy by enacting the Privacy Act, 1974 and Data Protection Act, 1998 respectively. But, now they

should seriously think about the protection of Individual Privacy and should legislate accordingly.

**6)** Data Privacy is a serious issue in the present social scenario. India should seriously think over the matter now. It has drafted "The Personal Data Protection Bill, 2018", which is a contemporary legislative initiative no doubt, but now it should be passed into an Act in order to define Personal data clearly and to prevent the loss of Personal Data by way of providing strict punishment.

**7)** 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.

**8)** In U.S.A., Health and Medical Privacy is protected by the Health Insurance Portability and Accountability Act, 1996 upgraded by the Health Information Technology for Clinical and Economic Health Act, 2009. But in India is lacking such type laws, passing of which is the urgent need of the hour herein. So, it's necessary to draft such type of law that's protect the health and medical privacy.

**9)** Data protection and privacy rights are two of the most important rights conferred by any civilized nation. Every individual and organization has a right to protect and preserve her/its personal, sensitive and commercial data and information. This is more so regarding health information and details that is required to be kept secret by laws like Health Insurance Portability and Accountability Act of 1996 (HIP A A) in United States. India does not have a dedicated law like HIPPA and presently HIPPA compliances in India are not followed. Similarly, we have no dedicated medical privacy law in India that can safeguard the sensitive health related information of the patients. In short, we have no dedicated data protection laws in India, data privacy laws in India and privacy rights and laws in India.

**10)** Both U.S.A. and U.K. have laws relating to protection of Data Privacy. But, in India there are is lacking such laws. The data privacy is regulated by different legislations like Information Technology Act, 2000, SPDI Rule, Credit Information Companies (Regulations) Act 2005, Indian Telegraph Act, 1885,

Telecom Regulatory Authority of India act, 1997, etc. Hence, time has come for India to enact a fresh law for protection of data privacy.

**11)** Right to Privacy has recently been declared as a Fundamental Right under Article 21 of the Indian Constitution by the Supreme Court of India in the Justice K.S. Puttaswamy v. Union of India case. But the Aadhaar-Privacy matter is still pending before the Five-Judge Bench of the Supreme Court. In this respect, Suggestions may be provided that, Aadhaar Card should be introduced for the prevention of terrorism and other fraudulent activities, but it should not convert our society into a surveillance society. Government should take appropriate steps for prevention of disclosure of personal information to any person by the introduction of Aadhaar Card System. The Aadhaar Act should incorporate strict punishment for the violation of Right to Privacy of Individual persons for the application of Aadhaar System. Storing and processing of personal data in the Aadhaar System should be kept in the hands of the government and distribution of such activities to large scale private organizations should be avoided. Unauthorized use of those personal data should be prevented by law. Linking of Aadhaar Number should not be made compulsory, except the matters of emergent concern. Supreme Court of India should provide extensive guidelines in this respect.

**12)** 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.

**13)** Government should authorize the proper agencies for data collection.

**14)** Government must ensure that proper agency which are authorized by government follow the regulation by doing periodic audit.

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

**16)** 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.

**17)** 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.

**18)** 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.

**19)** Government draft Retention policy of personal data and sensitive personal data must be specified and clear.

**20)** 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.

**21)** After the collections of our personal data and sensitive personal data our personal data and sensitive personal data are process by the Data Processor. Data processor processes our data independently or on behalf of the Data Controller. So, its required that we appoint Data Processor to that person which is skillful and knowledgeable on data privacy area.

**22)** Data controller is that who determine that for which purpose and what is the manner to processing of personal data of the individuals. So, its required that data controller have capacity to determine the manner and purpose of data processing. So, its required that we appoint Data Controller to that person which is skillful and knowledgeable on data privacy area.

**23)** 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.

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

**25)** E-governance is a good concept for governance. But there are unique privacy challenges associated with e-governance due to large storage of personal and sensitive data. Obviously, e-governance has given new dimension to development and globalization but there should be systematic improvements in governmental privacy leadership; and other technology-specific policy rules limiting, how the government collects and uses personally identifiable information. Government also has unparalleled opportunity to lead by example, by establishing strong, consistent rules that protect citizens without harming the government's ability of functioning. To achieve the specified goal, we have to adopt the fallowing measures,

a) Creating a Union Chief Privacy Officer
b) Installing chief privacy officers (CPOs) at all major departments
c) Strengthening and standardizing privacy notices including "privacy impact assessments
d) Ensuring that Data Mining techniques are addressed by the Privacy Act
e) Privacy Protection on agency website
f) Complaint processing in case of breach of privacy

**26)** Indian economy majorly based on e-business outsourcing. We need a privacy framework purely focused on e-business and cover privacy issues and provide legal assistance in case of any fraud, crime .Issues that are need to cover under privacy framework like proper storage of sensitive credentials like credit card,

safe credit of money during online transaction, Confidentiality, Integrity availability, authentication of party must be ensured before beginning of transaction, Encrypt the data before transmission of sensitive information, Restrict access based on need to know basis, assign unique identification to the parties that are involved in the business for authentication purpose. Also maintain the policy that addresses e-business privacy.

**27)** The collection of personal information by means of a surveillance system is lawful and justifiable as a policy choice, and if so, it must be ensured how privacy protective measures can be built into the system. "Reasonable expectation of privacy" is one of the keys to surveillance being legal. Using surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements. The activities like Access, Use, Disclosure, Retention, Security and Disposal of Surveillance Records must be regulated.

a) Prior to adopting a proposed surveillance program/practice an assessment of the impact on privacy is necessary
b) Public bodies should consider public consultations prior to introducing surveillance and inform those impacted once adopted
c) The design and operation of surveillance program/practice should minimize privacy intrusion to what is absolutely necessary to achieve its goals like designing and installing Surveillance Equipment
d) System operators require privacy-sensitivity training For National Security purpose this definition assumes to be optimism.

**28)** Surveillance is a matter of preserving national security, heritage, culture and life of each citizen. When we talk about national security with privacy concern then it is more focused on the safeguard of country sensitive information, agreement and security policies. Privacy of national security can be breached when espionage like activity can be performed by an individual to harm the reputation of the country. With respect to national security there is exemption of privacy from it. Must have separate framework with proper defined national security privacy guidelines. It must include that the government has authority

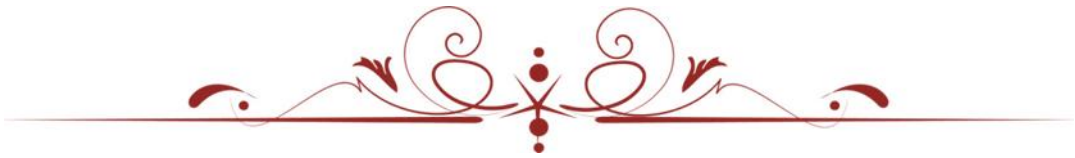
to investigate about any citizen, can seize any personal information regarding an individual when it mounts to National Security, because it is primary and foremost concern. Authority can access information anytime whether it belongs to private and public interest if they found susceptible or threat to national security. It has overall authority as it is deal with the preservation of millions of lives.

**29)** It is required that in present time drafting Data protection law on the basis of EU Laws.

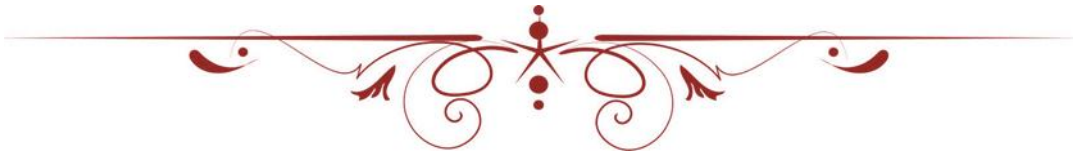
**30)** It is required that Constitute data privacy protection tribunals in every state, and district level for speedy justice.

**31)** However, despite the importance of these fields, till now we lack legal frameworks in the fields of data security, data protection and privacy protection. We urgently need to formulate data protection law in India and privacy laws in India. At the policy level as well privacy rights and data protection rights have been ignored in India. In fact, an Indian national privacy policy is missing till now. Even legislative efforts in this regard are not adequate in India. A national privacy policy of India is urgently required.

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



# *Bibliography*



# Bibliography


**1. Acts and Bills:**

- Aadhaar (Data Security) Regulations, 2016
- Aadhaar (Sharing of Information) Regulations, 2016
- Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act-2016
- Banking Companies (Transfer and Acquisition of Undertakings) Act, 1970 (Act No. 5 of 1970)
- Credit Information Companies (Regulation) Act, 2005 (Act No. 30 of 2005)
- Credit Information Companies Regulations, 2006
- Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
- Indian Telegraph Act,1885 (Act No. 13 of 1885)
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011
- Information Technology Act,2000 (Act NO. 21 of 2000)
- Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015
- Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017
- State Bank of India Act,1955 (Act No. 23 of 1955)
- The Data (Privacy and Protection) Bill, 2017
- The Mental Health Act, 1987" (Act No. 14 of 1987)
- The personal Data Protection Bill, 2014,
- The Personal Data Protection Bill, 2018
- The Public Financial Institutions (Obligation as To Fidelity and Secrecy) Act, 1983" (Act No. 12 of 1983).
- The Right to Privacy of Personal Data Bill, 2016

**2. Conventions and treaty:**


- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001
- APEC Privacy Framework, 2015
- Asia Pacific Economic Corporation Privacy framework 2004
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981
- Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981
- EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data 1995
- European Community Directive on the Protection on the Individuals with Regards to the Processing of Personal Data and Free Movement of Such Data
- European Convention on Human Rights
- International Covenant on Civil and Political Rights, 1966
- Organization for Economic Corporation and Development Guideline Governing the Protection of Privacy and Tran-Border Flows of Personal Data 1980
- Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 1980
- Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, (2013)


## 3. Books:


- Ausloos Jef, "The Right to Erasure in EU Data Protection Law" Oxford University Press United Kingdom, 2019
- Bainbridge, David "Data Protection Law" Universal Law Publications, Delhi, 2007
- Brkan Maja, "Courts, Privacy and Data Protections in the Digital Environment" Edward Elgar Publications United Kingdom, 2017

- Bygrave, Lee A. “Data Privacy Law: An International Perspective” Oxford University Press, United Kingdom,2014
- Denis Kelleher and Murry Karen “EU Data Protection law” Bloomsbury Publications United Kingdom, 2018
- Durga Das Basu, Comparative Constitutional Law (1984)
- Fuchs, Christian “Social Media: A Critical Introduction” Sage Publications, London, 2017
- Halinun Dara, “Data Protection and Privacy: Data Protection and Democracy” Bloomsbury Publications, United Kingdom, 2019
- Ismail, Noriswadi and Lee, Yong Cieh Edwin, et. at (eds.), “Beyond Data Protection” Springer Press, London, 2013
- Kothari, C.R “Research Methodology Methods and Techniques” New Age Publications New Delh,2014
- Kuner Chirstopher, “Transborder Data Flow and Data Privacy Law” Oxford University Press United Kingdom, 2013
- Lambert Parul, “A User Guide to Data Protection: Law and Policy” Oxford University Press United Kingdom, 2018
- Lee A. and Christopher Docksey “The EU General Data Protection Regulations: A Commentry” Oxford University Press United Kingdom, April 2020
- Lipschultz, Jeremy Harris “Social Media Communication: Concept, Practice, Data, Law and ethics” Routledge Press, London, 2018
- Massey, Stephen,”The Ultimate GDPR Practitioner Guide” Fox Red Risk Publication, United Kingdom, 2017
- Pandalai Shruti, “The Social Media Challenge to National Security: Impact and Opportunity” Institute for Defence Studies and Analyses, New Delhi, 2016
- Ronald E. Leenes, “Data Protection and Privacy: The Internet of Bodies” Bloomsbury Publications, United Kingdom, 2019
- Sathe,S P , “Right to Know” ,N.M.Tripathi,Bombay,1991
- Seervai, H. M. “Constitutional Law of India”, 2nd ed. N. M. Tripathi, Bombay,1975
- Singh, M.P: Comparative Constitutional Law, Eastern Book Company, 1989

- Singh, Rattan, “Legal Research Methodology” Lexi Nexis Publication, Nagpur, 2016
- Singhvi, L. M: Horizons of Freedom, New Delhi, National Publishing House, 1969.
- Sinha, B.S: An Introduction to Law of Torts through Indian cases, Eastern Book Company, Lucknow 1999
- Sinha, Manoj Kumar: Implementation of Basic Human Rights, New Delhi, Manak Publication Pvt. Ltd., 1999.
- Stewart, Daxton R., “Social Media and the Law” Routledge Press, London,2017
- Swarup, Jagadish: Human Rights and Fundamental Freedoms, N. M. Tripathi Private Ltd, Bombay,1975
- Tripathi, P.K: Spotlight on Constitutional Interpretation, N.M Tripathi Pvt Ltd, Bombay,1972
- Witzleb, Normann and Lindsay, David, “Emerging Challenge in Privacy Law” Cambridge University Press, London, 2014
- Wong Holen, “Cyber Security: Law and Guidence” Bloomsbury Publications, United Kingdom, 2018
- Zeller Bruno and Trakman Leon, “Data Protection Law: Comparative Analysis of Asia-Pacefic and European Approaches” Springer Press, Singapore, 2019


**4. Articles:**


- Akashdeep Bhardwaj and Vinay Avasthi, “Impact of Social Networking on Indian Youth - A Survey” International Journal of Electronics and Information Engineering, Volume 7, Issue 1, September (2017)
- Bishnu Prasad Dwivedi, "Right to Privacy: A New Horizon," All India Reporter, Aug 1991, Vol. 78, pp. 113-119.
- Brij Pal, "Right to Privacy and its Development in India," M.D.U. Law Journal, 2001, Vol. 6, pp. 171-80.
- Chetan Nagendra, "Privacy and the Concept of Data Protection in India," Chartered Secretary, July 2003, Vol. 33, pp.205-06

- D. S. Chauhan, "Data Surveillance, Privacy and Public Administrators," Indian Administrative and Management Review, Jan-Mar. 1976, Vol. 8, pp. 1-14.
- Dhrismitha Goswami, "Right to Privacy: In the Perspective of the Information Technology Act, 2000", Guwahati Law Times, April 2005, Vol. 2(1), pp. 1-14.
- Dilbir Kaur Bajwa, "Right to Privacy - Its Origin and Ramifications", CMLJ, (1990), Vol. 26.
- F. S. Nariman, "Right to be Let Alone", The Indian Advocate (1977), Vol. XVIII.
- Govind Mishra, "Privacy and the Indian Legal System", Delhi Law Review, 1990, Vol. 12, pp. 46-83.
- Govind Mishra, "Privacy as Public Issue", Vidhura, June, 1981.
- Govind Mishra, "Privacy: A Fundamental Right under the Indian Constitution," Delhi Law Review, 1979-82, Vol. 8 and 9, pp. 134160.
- H. R. Khanna, "Intercepting Letters: Invasion of Right to Privacy," The Statesman, September 15, 1981
- Jayashree, "Right to Privacy of a Woman under Criminal Law", Criminal Law Journal, May 2003, Vol. 109, pp. 145-49
- K. Pattibhi Rama Rao, "Right to Privacy: A New Fundamental Right," Andhra Law Times, 1999, Vol. 2, pp. 16-18.
- L. Jayanta Ghosh “Data Protection & Privacy Issues in India” Economic Laws Practice 03 (2017)
- M. K. Bhandari, "Right to Privacy Versus Freedom of Press: Comparative Conspectus of Legal Position in USA, US and India," Indian Journal of Legal Studies, 1991, Vol. 11, pp. 178-91.
- M. L. Upadhyay and Prashant Jayaswal, "Constitutional Control of Right to Privacy," Central India Law Quarterly, Jan-Mar. 1989, Vol. 11, pp. 39-58.
- M. V. Prashad Rao, "Right to Privacy - Palsied or Gauntlet", Andhra Law Times, 1999 (2), Vol. 97, pp. 16-18.
- Madhavi Divan, "Right to Privacy in the Age of Information and Communications," Supreme Court Cases, 2002, Vol. 4, pp. 12-23.
- Naveen Thakur, "Right to Privacy: An Implicit Fundamental Right Under Article 21," All India Reporter, Sep 1998, Vol. 85, pp. 145-46.

- Nemika Jha, "Legitimacy of the Right to Privacy as a Fundamental Right: A Comparative Study of India and America", AIR 2001, Journal Section, pp. 325-331
- P. Krubhala and P. Niranjana, "Online Social Network - A Threat to Privacy and Security of Human Society" International Journal of Scientific and Research Publications, Volume 5, Issue 4, April (2015)
- Rahul Saha and Surya Bala, "Sex, Property and Privacy: Testing and Constitutionality of Section 497,1.P.C", Criminal Law Journal, May 2005, pp. 156-60.
- Ruchika Agrawal, "Privacy and Technology: Are Indian Laws Catching Up", Lawyers Collective, 2004, pp. 17-19.
- S. B. Dawarkanath, "Right to Privacy: A Need for Constitutional Status," Andhra Law Times, 2002, Vol. 5, pp. 42-45.
- S. N. Parikh, "Telephone-Tapping and Right to Privacy," Gujarat Law Herald, 1998, Vol. 8, pp. 12-24.
- Satyam S. Irani, "Right to Privacy Inherent Freedom", AIR 2004 (Journal Section), pp. 26-27.
- Saurabh Awasthi, "Privacy Laws in India: Big Brother is Watching You," Company Law Journal, 2002, Vol. 3, pp. 15-23
- Suresh Kothari, "The Personal Data Protection Bill, 2018 Key Features and Implications" Indus law (August 2018)
- Survrajyoti Gupta, "Constitutionality of Wiretap in India and USA", Criminal Law Journal, December 2003, Vol. 109, pp. 379-83.
- Uday Shankar, "Privacy and Data Protection Laws in India: A Right Based Analysis" 21 Bharti Law Review 55 (2016)


**5. Newspaper and Magazines:**

- Frontline
- The Hindu
- The Hindustan Times, Lucknow
- The Times of India, New Delhi

**6. List of Websites:**

- Hein Online
- http://conventions.coe.int/Treaty/EN/cadreprincipal.htm
- http://csc.lexum.umontreal.ca/en/

- http://droit.francophonie.org/
- http://harvardhrj.com/
- http://indiacode.nic.in/
- http://nhrc.nic.in/
- http://www.altlaw.org/
- http://www.austlii.edu.au/legis/cth/consol/act/
- http://www.bailee.org/uk/cases/UKSC
- http://www.bailii.org/uk/cases/UKPC/(1879-2009)
- http://www.canlii.org/en/
- http://www.courtnic.nic.in/ordersmore.htm
- http://www.findlaw.com/casecode/supreme.html
- http://www.indiancourts.nic.in/
- http://www.indiankanoon.org/
- http://www.judis.nic.in/supremecourt/chejudis.asp
- http://www.law.cornell.edu/supct/
- http://www.lawcommissionofindia.nic.in
- http://www.statutelaw.gov.uk/
- http://www.texaslrev.com/
- http://www.worldlii.org/au
- http://www.yalelawjournal.org/current-issue.html
- JSTORE
- LexisNexis
- Manupatra
- SCC Online
- Westlaw International
- www.advocate.com
- www.hrc.org
- www.privacilla.org
- www.un.org/Overview/rights.html

**7. Dictionaries**

- Black's Dictionary
- Encyclopedia Britannica (Edition 1969)
- Everyman's Encyclopedia (Edition 1978)
- Human Rights Encyclopedia (Second Edition)
- International Encyclopedia of the Social and Behavioral Sciences (Edition 2001)
- The Encyclopedia Americana (Edition 1984)
- The Shorter Oxford English Dictionary, Vol.1, 1973

# *Annexure*

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

Myself **Arun Kumar Mishra**, Research Scholar, Department of Law (SLS), BBAU, Lucknow. I am doing research work under the supervision of **Prof. Priti Saxena**, Department of Human Rights (SLS) BBAU, Lucknow. My research topic is "***A Study on Judicial Trends in Privacy Law with Special Reference to Data Protection*".** For fruitful research work I need some useful data, so I request you to please fill up my questionnaire carefully and give me suggestion's if you want.

## About you

Name…….. Age……. Gender: Male / Female

Course: - UG/PG/Research Scholar Designations: - Assist. Prof./Associate Prof./Professor

## Questionnaire

Q. 1- Do you use Internet?

Ans. 1. Yes ☐ 2. No ☐

Q. 2- Do you know about how to use Internet?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know…….....

……

……

……..

Q.3- For what purpose do you use Internet? (Please tick in the box)

Ans.

a. Information ( )
b. E-mailing ( )
c. Social networking sites ( )
d. Professional use ( )
e. Instant messaging ( )
f. Gaming ( )
g. Photo and video sharing ( )
h. To Use of social media ( )
i. Online shopping ( )
j. Education ( )
k. Entertainment ( )
l. Downloading Music and video ( )
m. Other purpose ( )

If other purpose please mention……

……

……

……

Q.4 – Do you have an Account on Social Networking Sites? ( as Facebook, Twitter, My Space, etc.)

Ans. 1. Yes ☐ 2. No ☐

Q.5 – How did you come to know about Social Networking Sites?

Ans. 1. Family ☐ 2. Friends ☐ 3. Self ☐

Q. 6 - How Frequently do you use Social Networking Sites?

Ans. 1. Daily ☐ 2. Bi-weekly ☐ 3. Weekly ☐

4. Occasionally ☐

Q. 7 - How much time do you spend on Social Networking Sites?

Ans. (a) 0-1 hours ☐ (b) 1-2 hours ☐ (c) 2- 5 hours ☐

(d) More than 5 hours ☐

Q.8 - Which Social Networking Sites You Access? (Please tick in the box)

Ans.

a. Twitter ( )
b. Facebook ( )
c. YouTube ( )
d. My space ( )
e. Linked In ( )
f. Google Plus+ ( )
g. Orkut ( )
h. Instagram ( )
i. Pinterest ( )
j. Any other ( )

If you use any other sites please mention……

……

……

……

Q.9- For what purpose do you use Social Networking Sites? (Please tick in the box)

Ans.

a. Get connected with people ( )
b. Share information with friends ( )
c. Share photos and videos ( )
d. Entertainment ( )
e. Political purpose ( )
f. For publicity ( )
g. To know about others cultures ( )
h. To from public opinion ( )
i. Other purpose ( )

If you use social networking sites for other purpose please mention……..

……

……

Q. 10- When you use Social Networking Sites then do you read carefully Data Privacy policy?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

To what extent? .....

.....

.....

.....

Q.11- Do you know about Privacy?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know .....

.....

.....

.....

Q. 12- Do you know, in case of **Justice K.S. Puttaswamy (Ret.) and others Vs. Union of India and others**, Supreme court of India decided that "Right to Privacy" is a fundamental right?

Ans. 1. Yes ☐ 2. No ☐

Q.13- - Do you know about Data Privacy?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know ……..

……

……

……

Q.14- Do you assume that Indian judiciary plays a vital role for the protection of data privacy?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much it plays a vital role .....

.....

.....

.....

Q.15- Do you know about “Sensitive Personal Data”?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know

……

……

……

Q. 16- Do you share Your Aadhaar Number to any social welfare scheme/ Bank / fill-up examinations form, etc.?

Ans. 1. Yes ☐ 2. No ☐

Q. 17- Do you assume that your personal data and Aadhaar number which is share to any social welfare scheme/ Bank / fill-up examinations form, etc. are safe?

Ans. 1. Yes ☐ 2. No ☐

Q.18- Do you know about your rights related to the Data Privacy?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know ……

……

……

……

Q. 19- Do you know about “The Personal Data Protection Bill, 2018”?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know ……

……

……

……

Q. 20- Do you know about the “General Data Protection Regulations” (GDPR)?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know ……

……

……

……

Q.21- Do you know, where would you go for remedies, in case of breach of data privacy?

Ans. 1. Yes ☐ 2. No ☐

Q.22- Do you know, what are remedies available when any one breach your data privacy?

Ans. 1. Yes ☐ 2. No ☐ 3. To some extent ☐

If some extent,

How much you know ……

……

……

……

⇨ **Any suggestions** ……..

**……**

……

……

……

……

……

……

***Thank you***