COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS: A SPECIAL FOCUS ON THE UNITED STATES, UNITED KINGDOM AND INDIA

Dissertation submitted to National Law University and Judicial Academy, Assam

in partial fulfilment for award of the degree of

MASTER OF LAWS/

ONE YEAR LL.M. DEGREE PROGRAMME

Submitted by

K. Rahul Singha

UID: SM0222013

1 Year & 2nd Semester

Supervised by

Dr.Thangzakhup Tombing

Assistant Professor of Law

National Law University and Judicial Academy, Assam

CERTIFICATE

This is to certify that **K. RAHUL SINGHA** has completed his dissertation titled **"COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS: A SPECIAL FOCUS ON THE UNITED STATES, UNITED KINGDOM AND INDIA"** under my supervision for the award of the degree of MASTER OF LAWS/ ONE YEAR LL.M DEGREE PROGRAMME of National Law University and Judicial Academy, Assam

Date:

Dr.Thangzakhup Tombing
Assistant Professor of Law
National Law University and Judicial Academy, Assam

DECLARATION

I, **K. RAHUL SINGHA**, do hereby declare that the dissertation titled "**COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS: A SPECIAL FOCUS ON THE UNITED STATES, UNITED KINGDOM AND INDIA**" submitted by me for the award of the degree of MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME of National Law University and Judicial Academy, Assam is a bonafide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.

Date:

K. Rahul Singha
SM0222013
National Law University and Judicial Academy, Assam

ACKNOWLEDGEMENT

I thank Almighty for his countless blessings. This dissertation is the result of the pertinent efforts and contributions of many a people around me. I have taken sincere efforts to complete the dissertation, enjoying most of the research works, finding clueless amidst and finally relieved, proud and content to complete it. First, I would like to thank Dr.Thangzakhup Tombing for his guidance and support. I have been going through a hard phase if it was not for his kindness, patience and encouragement, the dissertation would have remained incomplete. I am deeply indebted for the consistent efforts Sir has taken for widening my perception and improving my work.

I would also like to convey my thanks to the Librarian, Officials, System Administrator and Staff of the NLUJA Library, Guwahati for their timely assistance to carry out the work.

Words fall short to express my love and gratitude to my parents, friends and family members for sticking through my side all the way. I feel blessed to have this circle of well- wishers who have always known ways to keep my spirits high.

Date:

K. Rahul Singha

UID: SM0222013

National Law University and Judicial Academy, Assam

TABLE OF CASES

31. State v. N.M.T. Joy Immaculate

32. Subhranshu Rout v. State of Orissa

33. United States v. Jones

34. Wolf v. Colorado

35. 'X' v. Hospital 'Z'

36. Zulfiqar Ahman Khan v. M/s Quintillion

TABLE OF STATUTES

TABLE OF ABBREVIATIONS

1.	&	And
2.	AIR	All India Reporter
3.	Anr	Another
4.	Art	Article
5.	CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
6.	CFAA	Computer Fraud and Abuse Act
7.	COPPA	Children's Online Privacy Protection Act
8.	CRA	Consumer Reporting Agency
9.	Del	Delhi
10.	DPA	Data Protection Act
11.	DPD	Data Protection Directive
12.	DPI	Digital Platforms Inquiry
13.	e.g.	Example
14.	ECPA	Electronic Communications Privacy Act
15.	ed.	Edition
16.	etc.	et cetera
17.	EU	European Union
18.	FCRA	Fair Credit Reporting Act
19.	FERPA	Family Education Rights and Privacy Act
20.	GDPR	General Data Protection Regulation
21.	GLBA	Gramm-Leach- Bliley Act

22.	GPS	Global Positioning System
23.	Guj	Gujarat
24.	HC	High Court
25.	HIPAA	Health Insurance Portability and Accountability Act
26.	ICCPR	International Covenant on Civil and Political Rights
27.	ICO	Information Commissioners Office
28.	IoT	Internet of Things
29.	J.	Judge
30.	Kar	Karnataka
31.	Ker	Kerala
32.	OECD	Organisation for Economic Co-operation and Development
33.	Ori	Orissa
34.	Ors	Others
35.	Pg	Page
36.	SC	Supreme Court
37.	SCC	Supreme Court Cases
38.	UDHR	Universal Declaration of Human Rights
39.	UK	United Kingdom
40.	UN	United Nations
41.	UOI	Union of India
42.	UP	Uttar Pradesh
43.	USA	United States of America
44.	v.	versus

Contents **page**

CHAPTER-1

INTRODUCTION

1.1 INTRODUCTION

Art. 21 of the Constitution of India considers right to privacy as an essential part of the right to life and personal liberty.[1] Justice Brandeis emphasized the importance of privacy by stating that in modern times, the need for solitude and privacy has become even more crucial for individuals. However, advancements in technology and business have resulted in violations of an individual's privacy causing significant mental distress which is worse than physical harm. A person's inalienable right to privacy expresses their inviolable personality and serves as a fundamental guarantee of their freedom and independence from any outside interference.[2]

In his book, "Digital Data Collection and Information Privacy Law"[3], Mark Burdon explains how smart devices are increasingly becoming a part of our daily lives. The "Internet of Things" is creating sensor based environments in our homes, workplaces and cities making them smarter and more efficient. This technology has the potential to provide numerous benefits including safer living environments, personalized experiences and improved resource management. Our homes will be able to understand our needs and adjust resources accordingly while personal devices will be able to track our behavior and mood to anticipate our future needs. Overall, the smart world has the potential to improve our quality of life significantly.[4]

In the era of cyberspace, information is readily available to anyone and users can easily upload and store data indefinitely. This data which includes social media activity, tweets, photos and online preferences is collectively known as our digital footprint. The increasing use of cyber technology globally has led to the adoption of e-commerce, e-governance, e-learning, e-courts and other digital services that make our daily lives more convenient. However, the rise of Big Data and algorithmic monitoring of online activity also raises legal questions about how data

[1] Justice K.S. Puttuswamy v Union of India, (2017) 10 SCC 1, 262
[2] Warren and Brandeis, The Right to Privacy, 5 Harvard Law Review, 193 (1890)
[3] Mark Burdon, Digital Data Collection And Information Privacy Law, (Cambridge University Press, 2020)
[4] Ibid

is collected, used, stored, accessed, handled and disposed of particularly with regards to the right to privacy in the cyber realm.[5]

Section 43A which comes under the IT Act states that a body corporate is accountable under for any confidential private information or data that it handles in an electronic system that it owns, controls, or manages. They are required to pay compensation to those affected. The IT Rules 2011 aim to safeguard individuals confidential data or information. Any individual or organisation who gathers, acquires, receives, holds, keeps, interacts with or manages confidential private information or data is required to produce a privacy policy for managing and dealing with such data. They must also make the policy available to those who provide such information under lawful contract.[6]

Protecting sensitive and individually identifiable information against unauthorised access, use or disclosure is known as data privacy. This information may include personal details. As more and more people and corporations acquire and keep personal information, privacy of data has become a crucial concern in the digital era.

The concept that people have the right to manage their own private information and to determine how it is used underlies the significance of data privacy. Sensitive information that ends up in the wrong hands can be used for financial fraud, identity theft, and other types of cybercrime. Additionally, data breaches can also harm an individual's reputation or lead to discrimination or exclusion.

Businesses and organizations are also affected by data privacy concerns. They may face legal consequences and financial penalties if they fail to comply with data protection laws or if their customers data is compromised. Data breaches can also damage a company's reputation, erode customer trust and lead to lost revenue.

To protect data privacy, individuals and organizations must take appropriate measures to secure their data. This includes implementing strong passwords and encryption, limiting access to sensitive information, and using secure networks and servers. Organizations must also comply with data protection laws such as the GDPR.

[5] Dr. Jasmine Alex,Privacy in cyber space., Livelaw, https://www.livelaw.in/columns/privacy-in-cyber-space-157769 accessed on 27 April 2023

[6] Rule 4 of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Individuals must also be aware of the dangers involved with disclosing confidential data online. They should only provide sensitive information to reputable organizations and avoid using public Wi-Fi networks or unsecured websites. Individuals can also take steps to protect their privacy such as adjusting their social media privacy settings using anti-virus software and being cautious about clicking on suspicious links or downloading unknown files.

In summary, data privacy refers to protecting personal and sensitive data from uncertified access, use or leakage. It is important for individuals and society to take appropriate measures to secure their data and comply with data protection laws. Being aware of the risks associated with sharing personal information online can also help individuals protect their privacy.

1.2 STATEMENT OF PROBLEM

With different countries such as the UK and the USA implementing its legislation in order to deal with the problems caused by fast paced change in technology. Simultaneously, data privacy laws also continues to evolve throughout the world over the decades. But despite of it, India lags in developing effective legislation on data privacy that safeguards private data as well as rights for individuals in the age of the internet. Although India has gone through numerous attempts to enact laws to safeguard data, these efforts have either not been passed into legislation or have not properly safeguarded the personal information of individuals till date. The Digital Personal Data Protection Bill (2022), a recently introduced measure of Indian laws includes several enhancements over earlier initiatives. Yet, there are still a few issues with the suggested legislation which would limit the safeguarding of information to a specific form which would render enforcement more difficult. Since, there is no adequate regulation for circumstances like identity theft, unauthorised usage of confidential information occurs. Due to inadequate regulations, technology experts violate others privacy and engage in discriminating behaviour. Therefore, the data protection law is essential for protecting our private information.

1.3 LITERATURE REVIEW

The researcher has read several books and articles for conducting the research. The researcher found several of them to be pertinent including the following.

- **Mark Burdon, Digital Data Collection and Information Privacy Law**

In his book *"Digital Data gathering and Information Privacy Law",* Mark Burdon argues that the law should be updated to address the new power implications of widespread collection of data. It discusses the business models which rely on databases of data from sensors with a special focus on smart homes. Burdon highlights the problems confronting the control-model for data security and its enactment of essential measures for the transmission of private data. Burdon lays the basis for future changes in law and argues for better data security laws guarantees by identifying the primary function of person authority in data privacy as an interrupter of modulated authority.

- **Michael C. James, A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe**

This book highlights about the Americans who are from socioeconomic class that strongly support their right to privacy in a variety of instances. Considering the current Overseas Contingency Operation and some subsequent legislative matters and executive measures that have granted government agencies improved and increasingly intrusive, authority for monitoring as well as accessibility to generally private data, this subject has become particularly important for modern Americans by which the researcher gets a clear picture of right to privacy.

- **Brandeis and Warren's, The Right To Privacy and the Birth of the Right to Privacy**

In this book the author argued that legislation needed to recognise right to privacy and enforce tort liability on those who violate it. It also discusses about the Right to Privacy that received promptly and broad support since its developers expressed people's outrage at the pervasive aspects of growing urban life into a compelling and rational call for reform to the legitimate and legislative matters establishment.

- **Daniel J Solove, The Digital Person**

This book examines the societal, political and legal consequences of the storage and utilisation of private information in digital databases. This book addresses the issue from many approaches covering how businesses accumulate private data in large databases, how the authorities is progressively allowing companies access to this data via public databases and how the government obtains private data from companies for its own benefit.

- **Elif Kiesow Cortez, Data Protection Around The World-Privacy Laws In Action**

This book constitutes a summary of privacy legislation and practices from a variety of countries so as to render guidance. The researcher has also found specific information on privacy laws through this book, which is beneficial for conducting this research.

- **Christina P. Moniodis, Moving from Nixon to NASA: Privacy's Second Strand- A Right to Informational Privacy**

This article discusses about the two decisions by the Supreme Court dealt with data privacy issues and also the court's reluctance to enact privacy laws which may be owing to the non-rival, indistinct and regenerative characteristics of data that enables plaintiff's damage to evade courts.

1.4 AIMS

The aim of this research paper is to compare the data protection laws and regulations of the US, UK and India and to examine the effectiveness of the data protection laws in each country in terms of protecting individual's personal data and privacy.

1.5 OBJECTVES

The objectives of this research are as follows:-

- To examine the level of safeguarding for the right to privacy in the digital realm within India.

- To understand the different legal provisions in India concerning the safeguarding of an individual's privacy with regard to their personal data.
- To make a comparison between the legal structures established by different countries for safeguarding individual's privacy concerning their personal data on the internet.
- To understand the steps taken by the Indian laws to ensure the data protection.

1.6 SCOPE AND LIMTATIONS

- The study will show how the right to privacy has changed over time in India, particularly with regard to data security.
- The study promotes a global standard of data protection by analysing current legislation regarding data privacy in different countries.
- The study puts emphasis on how easily and frequently without awareness consent for the collection of information is acquired and argues that the existing "consent based" strategy should be replaced with a "right based" one.

The research is limited to the examination of privacy laws in cyberspace, the US and the UK are the only countries selected for a comparative study of data protection legislation in different jurisdictions. This is mostly because an effective legislative foundation governing information protection in cyberspace has been found in these three countries.

1.7 HYPOTHESIS

The privacy of people in relation to their personal information in cyberspace is not sufficiently safeguarded under Indian legislation.

1.8 RESEARCH QUESTIONS

- Whether current Indian legal system is effective in resolving the legal issue of data breaches?
- Whether India's data protection laws are as effective as those in the US and UK?
- Whether the existing consent based strategy should be replaced with a right based one?

- What significant measures will India take to guarantee that the privacy of people regarding their personal data is effectively protected?
- What are the legal approaches used in India to safeguard people's data privacy?

1.9 RESEARCH METHODOLGY

The researcher used a doctrinal research methodology. The library and other web sources served as the only basis for current study. Numerous books and articles of different types have been found to be helpful in obtaining sufficient information relevant to the current research. Many resources on the internet have been found to be very beneficial for an improved understanding of this area of study.

1.10 CHAPTERISATION

- **In the first chapter of this paper,** it deals with the introduction of this paper, statement of problem, Literature Review, Aims and objective, Scope and limitations, Hypothesis, Research methodology and Chapterisation.

- **In the second chapter of this paper,** it deals with the historical background of right to privacy and examines the concept of private data and its significance to development of privacy in India. The other international legislation, judgements from various nations and the Indian judiciary perspective are examined and analysed here.

- **In the third chapter of this paper,** this chapter aims to explain the details and history of the protection of data. The right to be forgotten and the right to erasure, both of which are in depth facets of data privacy are also covered here.

- **In the fourth chapter of this paper,** this chapter discusses laws governing data protection in the United States, United Kingdom and India.

- **In the fifth chapter of this paper,** conclusions and suggestions are discussed in the last chapter. The findings of the research are discussed as well as suggestions to implement a data protection mechanism in India.

CHAPTER-2

2. HISTORICAL BACKGROUND OF RIGHT TO PRIVACY

2.1 INTRODUCTION

The privacy concept, as it exists in the present day, is not a straightforward matter. Over time and across different nations and academic viewpoints, the definitions and concerns surrounding privacy have exhibited variations. Samuel Warren and Louis Brandeis provided a seminal definition of privacy in the late 19th century, stating that it was the right to be free from interference. However, this simplistic definition falls short in determining which specific aspects of an individual's personal life should be shielded from intrusion. For instance, there may be distinct realms of privacy like space privacy, behavioral privacy, decisional privacy and data privacy.

Although the American and Indian Constitutions do not explicitly mention privacy as a fundamental right or provide a definition for it, the courts in both countries have gradually acknowledged and interpreted privacy as an inherent aspect of fundamental rights through their judgments.

Initially, in India, the majority ruling in cases like *Kharak Singh*[7] rejected the idea of concept of privacy. Inspite of that, the court of law followed the approach of judicial activism seen in American legal system and began to interpret the constitution to recognize a fundamental right to privacy with the progress of time. This interpretation was founded on the principle of Art. 21. In Justice *K.S. Puttaswamy v. UOI*, the right to privacy is inherent and protected as a basic component of the right to life and personal freedom enshrined by Art. 21 of the Constitution, the Supreme Court decided.

2.2 ORIGIN OF RIGHT TO PRIVACY

The freedom human being have to manage their identities by themselve is directly related to their right to privacy. Its origin can be discovered back to the concept of natural or inherent

[7] AIR 1963 SC 1295

rights inherent in human beings. These natural rights are inseparable from human personality and cannot be taken away. They are essential for the functioning of human life. The ancient Greek philosopher Aristotle recognized a distinction including political matters in the public domain and the realm of individual human life suggesting an instant understanding of the necessity for a secure area for inhabitants.[8]

In his 1690 Second Treatise on Government, John Locke argues that people's lives, freedoms, and property are intrinsically personal and protected by basic natural law. This notion of a private preserve was established to establish boundaries against external interference. In his remark on the Laws of England written in 1765, William Blackstone discussed the concept of "natural liberty." He believed that absolute rights were granted to individuals by the unchanging natural laws and these rights included individual security, individual liberty and property rights. An individual's valid and unaffected enjoyment of their life, physique, health, body parts and dignity is included in their right to privacy and safety.[9]

According to Mill: According to mill: any person's social pressure is subjected by sole aspect of behaviour that affects others. In so far as it only acts on him, his sovereignty by nature and free from any sorts of restriction, the person is sovereign over oneself, over his own principles as well as his own thinking.[10]

The American Constitution's maker, James Madison, thought that safeguarding individuals rights and liberties was crucial and saw them as inherent and unalienable, much like the rights of property. Just as a person's land, goods and money are considered their property, Madison argued that individuals also have a property right in their opinions and the ability to freely express them. Furthermore, individuals have a vested interest in the unrestricted use of their abilities and the freedom to choose how to utilize them. In essence, just as a person is entitled to their property, they can also be said to have a property right in their rights.

Madison asserted that in a situation where excessive power dominates, no form of property is adequately respected. In such circumstances, individuals are not safe in expressing their opinions, safeguarding their personal well-being, utilizing their abilities or protecting their possessions. According to Madison, conscience is the most sacred form of property as it is a natural and inherent right that exists independently of positive law. While other forms of

[8] Michael C. James, A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe, 29:2, Connecticut Journal of International Law, 261 (Spring 2014),
[9] Justice K.S. Puttaswamy v. UOI, (2017) 10 SCC 1
[10] John Stuart Mill, On Liberty, 13, (Batoche Books 1859)

property may be subject to legal regulations, the exercise of one's conscience is a fundamental and unalienable right that should be protected.

Madison emphasized that protecting a person's home as their castle and ensuring the faithful fulfillment of public and private debts cannot justify infringing upon an individual's conscience. Conscience is deemed more sacred than one's dwelling and the duty to safeguard it should not be withheld. This responsibility derives from the very essence and underlying assumptions of the social compact that forms the basis of society.[11]

Samuel D. Warren and *Louis D. Brandeis* examined the concept of *"right to be let alone"* and the *"right to privacy"* in their paper *"The right to privacy"*. The authors argued that as civilization has progressed, the increasing intensity and complexity of life have made it necessary for individuals to seek retreat from the world. People who have been impacted by cultural development have evolved into creatures that are more susceptible to exposure in public. As a result, people now place a greater value on isolation and privacy.

However, the authors pointed out that modern advancements in enterprise and technology have intruded upon this privacy, causing individuals significant mental pain and distress. Such intrusions can inflict greater harm than mere physical injury. Personal writings and other private works are protected from publication but not against physical appropriation or theft under a basis that is unrelated to the idea of private property. Instead, it is motivated by the need to protect a person's eternal personality.

As a basis for the right to privacy which *Brandeis* and *Warren* introduce to as the 'Right to be left alone', they delineated a recognised legal right. This included the freedom for people to decide how much of their ideas, feelings, and private information is shared with others. The fundamental idea underlying this right was the preservation of an individual's inviolate personality[12]. In essence, the right to be let alone served as a safeguard against the unauthorized or involuntary exposure of private details, thoughts, emotions and similar aspects of one's life.[13]

[11] James Madison, Essay on Property, in Gaillard Hunt ed., 6 The Writings of James Madison 101-103, (1906).
[12] Bratman, B. E.: Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy,69 Tennessee Law Review 344 (2002)
[13] Prosser, W.: Privacy, 48:3 California Law Review, 384 (1960)

2.3 THE CONCEPT OF PRIVACY UNDER INTERNATIONAL LAW

The recognition and formalization of fundamental human rights marked a significant milestone in the human rights movement. Over time, human rights law has gained increased prominence in both local and global judicial arenas, particularly through the establishment of the United Nations which has made human rights a central focus of international law and politics. Several international and national agreements have explicitly acknowledged the privacy rights in various region. The universality that privacy is consistently involved in almost every people rights agreement or discussion reveals how essential it is.

The emergence of the 'Right to privacy' in modern jurisprudence of human rights occurred in 1948 with the inclusion of *"Article 12 in UDHR"*. Art. 12 states:

"Nobody shall be the target of willful intrusion into their personal space, those of friends and family, their homes, or their communications, or of incidents on their character or dignity. Everybody possesses a right to be safeguarded from these types of interference or violence".

This provision seeks to create a legal structure in the global arena that mandates nations to ensure both physical and communication privacy. It also aims to encompass a broad spectrum of human interactions and conduct. This involves defending one's family's privacy and right to reputation. Law regarding human rights law is widely recognized for its objective of nurturing human dignity and shielding it from unwarranted interference. Consequently, privacy takes centre stage as the key focal point in striving to achieve the objectives of human rights law.

"Art. 17 ICCPR" reaffirms the importance of privacy as stated in the *"UDHR"* and emphasizes the need for legal protection of this right.

1. Nobody shall be the victim of wilful or unlawful invasion into one's right to privacy, neither in home, family and communication, unwarranted assaults on one's own dignity nor prestige.

2. Everybody is entitled to lawful safeguard from such intrusion or assault.[14]

According to *"Art. 14 of the CRMW,"* a similar concept is employed to safeguard the rights of migrant workers. This provision aims to shield migrant workers and their families from unwarranted intrusion into their family life and privacy. Furthermore, both "*Art. 16 of the CRC*

[14] United Nations Office of the High Commissioner, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, visited on 24/05/23

and Art. 22 of the CRPD" specifically focus on securing the privacy of children and individuals with disabilities.

According to a report for human rights published by the UN High Commissioner on June 30, 2014, protecting a person's right to privacy in both law and practise is crucial because it is recognised by everyone as having fundamental significance and lasting relevance. This is especially true in the digital age.[15]

2.4 PRIVACY PROTECTIONS IN REGIONAL HUMAN RIGHTS CONVENTIONS

2.4.1. "EUROPEAN CONVENTION ON HUMAN RIGHTS 1950"

Privacy is a fundamental aspect of the European Convention on Human Rights (ECHR) as mentioned in Article 8.[16] In a democratic society, Right to privacy is not fixed and may be content to some restrictions. These exceptions must be defined by specific legislation enacted in this field. Authorities are not allowed to violate this right unless they do so in accordance with legislation that is required for a sovereign society for public safety, national safeguard or the health of the nation's economy, to stop violence or chaos, to secure health or to secure the rights and liberties of individuals as stated in Art. 8.

In specific situations, it is possible to bypass the requirements. It is crucial to remember, nevertheless, that the European Council Directive requires member states to develop data protection laws that adhere to the directive's principles. [17]

[15] "The Right to privacy in the Digital age", Report of the Office of the United Nations High Commissioner for Human Rights (30 June 2014).

[16] 8. Right to Respect for Private and Family Life. –
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[17] Directive 95/46/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 last visited on 25/05/23

2.4.2. "AMERICAN CONVENTION ON HUMAN RIGHTS, 1969"

Privacy has been given a significant importance in the ACHR.[18]

Article 11 states:

1. Every individual has the right of having their dignity safeguarded and respected.

2. Nobody should be the victim of illicit attacks on their dignity or personality or of arbitrary or violent intrusion with their family, residence, or correspondence.

3. Everyone has a right to legal protecting itself against these types of invasions and violence.

2.4.3. "African Charter of Human and People's Rights 1981"

In ACHPR, Right to privacy is not expressly stated but its importance is highlighted by Art. 18, which emphasises the state's duty to secure family livelihood.[19]

2.4.4. "African Charter on the Rights and Welfare of the Child, 1990"

Art. 10 of the charter states the right to privacy for children too. It further states that every child has the right. Every child has the right to be free from inappropriate or illegal invasions into their personal space, their family, their place of residence, or their interactions, as well as from attacks on their dignity or goodwill, as long as they or their legal guardians have the authority to exercise appropriate control over their behaviour. The child is entitled to legal protection from these types of interference or abuse.[20]

[18] American Convention On Human Rights "Pact Of San Jose, Costa Rica", 1967

[19] Article 18-

1. The family shall be the natural unit and basis of society. It shall be protected by the State which shall take care of its physical health and moral.
2. The State shall have the duty to assist the family which is the custodian or morals and traditional values recognized by the community.
3. The State shall ensure the elimination of every discrimination against women and also ensure the protection of the rights of the woman and the child as stipulated in international declarations and conventions.
4. The aged and the disabled shall also have the right to special measures of protection in keeping with their physical or moral needs.

[20] African Charter on the Rights and Welfare of the Child, 36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf accessed on 25/05/23

2.5 THE CONCEPT OF RIGHT TO PRIVACY IN INDIA

The 'Right to privacy' is not specifically brought up or guaranteed as a fundamental right in the Constitution of India. The Preamble's[21] content and the rules established in the Part III[22] of the Indian Constitution, however, both inferred that everybody shall have the right to privacy.

The following provides a detailed discussion on the different cases concerning the right to privacy and how the judiciary has reacted to them.

1. *M.P Sharma v. Satish Chandra*[23]

In a noteworthy case, the Apex Court, represented by a bench of the three-judge which addresses the jurisdiction of the CrPC governing forage and seizure denied the recognition of the Right to privacy.

There was no justification for merging it into a wholly other fundamental rights by a manner of weary build since authors of the Constitution chose against establishing a Fundamental Right to privacy similar to the Fourth Amendment in the [American] Constitution.

The Apex court pronounced that the challenged law is constitutional, affirming that the state possesses the ultimate authority to perform searches and seizures for the purpose of ensuring security.

2. *Kharak Singh v. State of U.P.*[24]

The plea filed to the supreme court challenges the credibility of Uttar Pradesh Police Regulations (Regulations 236 and 237) under chapter 22 as well as the discretion given to police personnel under its distinct provisions. The main argument against the limits is that they violate the rights that people are entitled to under Indian Constitutional Articles 19(1)(d) and 21.

[21] "liberty of thought, expression, belief, faith and worship" and "Fraternity assuring the dignity of the individual"
[22] Article 19 (1)(a)- Right to freedom of speech and expression, Article 19(1)(d)- Right to move freely throughout the territory of India, Article 21- Right to life and Personal Liberty
[23] AIR 1954 SC 300
[24] AIR 1963 SC 1295

The Court cited J. Frankfurter's remark in Wolf v. Colorado[25] that each person's privacy must be protected from arbitrary police involvement in a free society. As a result, it roughly falls under the idea of ordered freedom and can be used to oppose the state in a due procedure. On the grounds of banging on the gateway, even if it's night or day, served as an opening to a forage, with no licence of law but only having the jurisdiction of the police, it was not necessary for the opinions of the past to be explicitly criticised as being incompatible with the idea of human rights stipulated in historical records and the fundamental laws of English speaking peoples. We may state without doubt that the protection provided by state would be in violation of the Fourteenth Amendment if it deliberately encouraged such police violations of people privacy. The Court observed that it is obvious that the man's movement is not hindered or negatively affected in any way by a knock on the gate or the person being awakened while taking a nap. Hence it is not violation of Article 19 (1)(d). In accord with the evaluation of Regulation 236 under clause (b) distinctly breaches Article 21 and to hold it up there is no law enacted so it must be declared unconstitutional. In the decision emphasised by most of the judges present states that the Indian constitution does not specifically safeguard the right to privacy.

Justice *Subba Rao* in his dissenting judgement agreed with the belief that the Right to privacy may be taken from the idea of individual freedom as conveyed in Art. 21. According to Justice SUBBA RAO, the personal liberty right also includes having no restriction on one's movements or having no one's privacy violated. Individual liberties crucial component is the right to privacy, though the Indian constitution does not officially name it as a basic right. Domestic life is sacred in any democracy.

3. *Govind v. State of M.P*[26]

The Right to privacy was examined thoroughly by the apex court in the mentioned case. In this case the Supreme Court clearly analysed the M.P. Police (Regulations 855 and 856) credibility, which authorise various kinds of monitoring. In addition, the court established a restriction which was extracted from Art. 19(a), 19(d) and 21 on the fundamental right to privacy. Further the restricted basic Right to privacy extracted from the Articles was also acknowledged by the court. Therefore, it cannot be said that the right to privacy is not unrestricted, but under Article

[25] 338 US 25 (1949)
[26] AIR 1975 SC 1378

19(5), reasonable restrictions is imposed to safeguard the interest of the people at large. In the case of Govind, Justice Mathew made the following observation:

The Right to privacy needs to be expanded in any occasion on a case by case grounds. Henceforth, if the Right to free expression and Right to individual liberty and the liberty to move around India's territories sums up in a discrete Right to privacy which is a fundamental right it is not meant that this right is inalienable.[27]

MATHEW, J., also observed:

If a significant competing interest can be proven to be superior, dignity and privacy concerns should be carefully considered and only then should they be overruled. The significant State interest test must be met for a statute to be upheld by the Court as a grounded privacy rights.

4. *Malak Singh v. State of Punjab*[28]

In this case, the legality of some monitoring techniques used by the Punjab Police Rules was examined by the Apex Court. In that examination it was noted by the Apex Court that it was required for establishing a balance between individual liberty, dignity and personal freedom provisions by the Indian constitution under the Art. 19(1)(d) and 21 along with the objective of addressing violence and maintaining the safety of the public. It was determined that police monitoring should not encroach upon an individual's fundamental rights and although crime prevention is a legitimate public interest, surveillance conducted for this purpose should not be considered as "unlawful interference" in someone's life. The court emphasized that surveillance measures must be reasonably limited to fully respect and uphold an individual's fundamental rights. It was held that an individual basic liberties such as Article 21 of our Indian constitution which safeguards the individual freedom and particularly his or her liberty of movement are put at risk by intrusive monitoring which significantly invading their privacy.

[27] AIR 1975 SC 1378
[28] (1981) 1 SCC 420

5. *Peoples Union for Civil Liberties v. Union of India*[29]

This case concerns recent incidents of telephone tapping. Art. 32 of the Indian constitution was addressed by the organisation in an action in the people's interest. In Article 21, the Constitution guarantees the general right to individual freedom and life which involves the Right to privacy. The court of law emphasized that telephone tapping should only be employed by the government in exceptional circumstances such as a public emergency or when public safety is at stake. According to the ruling of the court, we do not hesitate to claim that the "right to privacy" is a component of the "right to life" guaranteed by Art. 21 of the Constitution of India. Article 21 is used when a right to privacy is proven by the situations of a specific case. The mentioned right cannot be curtailed unless a legal procedure is followed.[30]

The stated concerns regarding recent incidents of telephone tapping, the organisation in an action in the public interest under Article 32 of the Constitution, the NGO has challenged Section 5[31] as being illegal since it provides the governments the authority to tap phones in specific circumstances. The writ suit was submitted in reaction to the CBI's findings on the monitoring of politicians phones.

The Court set forth specific rules that govern the state's authority concerning phone taping and communications monitoring stipulated under Section 5[32]. These guidelines aim to safeguard the public interest and prevent the government from arbitrarily and unlawfully exercising its power. The Court has expressed dissatisfaction with the State's failure to establish norms that would prevent the abuse of authority thus far. It is difficult to safeguard the rights of people protected by Articles 19(1)(a) and 21 of the Constitution without a fair and just mechanism to regulate the use of authority under Section 5(2) of the Indian Telegraph Act. Only in the event of a public emergency or when it is in the best interest of public safety may the provisions of Section 5(2) of the Act be used. The government is lacking the power conferred by the law unless a citizen crisis has occurred or it is necessary for the safeguard of the people.[33] According to the verdict of the court, a public emergency is described as an unexpected event or situation that impacts the general public and requires immediate action. In contrast, public safety relates to an instance or situation whereby the general public is subjected to serious risk or threat. The Court emphasised that even if they believe it to be essential or advantageous for

[29](1997) 1 SCC 301
[30] Ibid
[31] Indian Telegraph Act of 1885
[32] Ibid
[33] Ibid

preserving the nation's sovereignty and integrity, the Central Government, State Governments, or authorised officials are not permitted to use telephone tapping if one of these elements is missing.

6. District Registrar and Collector, Hyderabad & Anr v. Canara Bank[34]

The apex court panel of two judge considered the credibility of particular laws of the Indian Stamp Act, 1899 (as amended by a special Andhra Pradesh legislature) in this case. The aforementioned provisions gave the officer in charge of collecting, or any other person authorised by the Collector, the right of entering the premises to review any books, documentation or records kept by public authorities. The inspection's goal was to find any instances of fraud or refusal to compensate the government for unpaid duties as needed by Section 73[35]

The privacy of consumer details maintained by financial organisations like banks was the key concern in this case. The Supreme Court determined that the challenged provision was unconstitutional because it did not adhere to the reasonable standards imposed by Articles 14, 19 and 21. The court found that any rule that restricts an individual's freedom of choice including the privacy of their financial information must fulfill the three essentials as in Maneka Gandhi[36] case outline by the Supreme Court.

The triple test necessitates that any law encroaching upon "personal liberty" under Article 21 must satisfy specific criteria.

(i) a process must be prescribed;

(ii) The method must adhere to any requirements of the fundamental rights listed in Article 19 that could be pertinent in specific situations; and

(iii) It should to be able to be examined in light of Article 14.

The provision in question was found to be unsuccessful in meeting this criterion. Most significantly, the court concluded that the notion of privacy pertained to individuals rather than specific locations. This assertion indicated that the physical storage of financial records, be it

[34] (2005) 1 SCC 496
[35] Andhra Pradesh Stamps Act.
[36] (1978) 1 SCC 248

at a person's residence or a bank was irrelevant. Financial records would be protected by the right to privacy as long as they belonged to a specific person.

7. *Hinsa Virodhak Sangh vs Mirzapur Moti Kuresh Jamat & Ors*[37]

The challenge was made to the validity of a resolution that imposed limitations on the operation of slaughterhouses for a brief period coinciding with a Jain festival. It was held that, Art. 21 of the Indian constitution guarantees a person's right to privacy which includes his or her freedom to decide whatever they like to consume.

8. *State of Maharashtra vs. Bharat Shanti Lal Shah*[38]

It involved a judicial examination of the legality of the Maharashtra Control of Organised Crime Act, 1999 (MCOCA). The specific sections of the Act under scrutiny were Sections 13 to 16 which pertain to the authorization of telephone tapping. The challenge was centered around the validity of these provisions. The Court found that overhearing discussions violates a person's right to privacy, but that this right may be limited in accordance with legal standards. As a result, the Court must make sure that the procedure is fair, rational, and devoid of any aspects of arbitrary behaviour or illogical reasoning.[39] According to the Court, these rules create a "procedure established by law" and include adequate procedural protections that prevent them from being unfair or arbitrary. This is because Section 16 imposes penalties on individuals who access information through the interception of wire, electronic, or oral communication[40] without authorization.

9. *Selvi v. State of Karnataka*[41]

The case investigates the legal issues surrounding the mandatory use of scientific techniques to aid in criminal investigations, such as narcoanalysis, polygraph testing, and the "BEAP" test. The court has come to its decision that these methods violate a person's inherent human rights

[37] (2008) 5 SCC 33
[38] (2008) 13 SCC 5
[39] Ibid
[40] Ibid
[41] AIR 2010 SC 1974

as the procedures are severe and violate the fundamental right to mental privacy if they are carried out violently. The judgement found that the involuntary application of these tactics breaches the Constitution's Article 20(3) guarantee against self-incrimination.

10. Ram Jethmalani v. Union of India[42]

The Apex Court considered a case involving secret funding that was of public interest. The case involved a plea to establish a Special Investigating Team (SIT) responsible for tracking and probing a trail of money. The court observed that social order is destroyed by an inquisitorial system when citizens fundamental rights to privacy are violated by other citizens. The concept of fundamental rights which involves the right to life and right to privacy goes wholly beyond the straightforward restriction against governmental violations. Additionally, even while such people are exercising fundamental rights, the state still has a duty to protect them from the actions of others in society. It held that Individual's rights to privacy would be violated if their bank account information was made public without first establishing that there was sufficient evidence to charge them with wrongdoing.[43]

11. Justice K.S. Puttaswamy v. Union of India[44]

In a landmark decision made by nine judge bench, the apex court has acknowledged privacy as a fundamental right. The court further emphasised that Right to privacy is not unqualified and that it might curtail in certain situations. Restrictions on privacy can be imposed if they are provided by law, serve a legitimate purpose of the State and are proportional to the objective they aim to achieve. Earlier judgements in the case of Kharak Singh and M.P. Sharma which denied the right to privacy constitutional protection were reversed by this verdict. The notion of informational privacy was addressed by the Supreme Court together with numerous regional and international privacy legislation. Speaking on behalf of the majority, Justice Chandrachud stated that "the right to privacy is equivalent to all other liberties protected by Part III of the Constitution." It is viewed as an inherent natural right and a crucial aspect of human dignity. However, Chelameswar J. describes the right to privacy as having three components including

[42] (2011) 8 SCC 1
[43] Ibid
[44] (2017) 10 SCC 1

personal decision (autonomy to make personal life decisions), sanctuary (protection from invasive observation), and relaxation (freedom from unwelcome stimuli).[45]

Justice Kaul notes that privacy concerns may be centred on both non-state groups or organisation. He also highlights the necessity of technology in the context of prevalent data collection, acquisition and utilisation in the cybernated economy while raising concerns about state monitoring and outlining. The impact of big data are also covered by Kaul J., including how it affects people's daily lives and how it could suppress the right to free speech and expression. He understands that as a conclusion private and public actors must be kept away from access of critical information.

2.6 PRIVACY: A COMPLEX RIGHT WITH MANY DIMENSIONS

A person's right to privacy includes various dimensions beyond the aforementioned legal cases primarily addressing state surveillance and interference. Additionally, several other aspects are examined and discussed as follows:-

2.6.1 PRIVACY OF THE PHYSICAL BODY

In Indian law, medical records are generally protected under the right to privacy. However, this protection is subject to certain limitations when it comes to the courts, as non-disclosure of these records could potentially pose a threat to the lives of other individuals.

In *X v. Hospital Z*[46], the Apex Court talk about the scope of a blood donor's privacy rights matter pertaining to their medical data. In this said case, the hospital staff conveyed that the blood donor was confirmed to have HIV without the donor's consent. This disclosure caused the donor's fiancée to end their engagement due to societal stigma. Although medical records are typically considered private, the Supreme Court ruled that doctors and hospitals can make exceptions in specific situations where withholding medical information could endanger the lives of others, in this instance, the wife to be. Consequently, the court legalized the disclosure as it was deemed necessary to protect another person's right to health.

[45] Bhandari, V., Kak, A., Parsheera, S., & Rahman, F., An Analysis of Puttaswamy: The Supreme Court's pivacy Verdict https://www.indrastra.com/2017/11/An-Analysis-of-Puttaswamy-Supreme-Court-s-Privacy-Verdict-003-11-2017-0004.html accessed on 30/05/2023
[46] (1998) 8 SCC 296

In *Sharda v. Dharmpal*,[47] The issue at hand was whether the Court has the authority to direct an individual to undergo a medical examination during matrimonial proceedings. According to the Apex Court, the privacy rights is not absolute. In this case, the disputing rights were the right to seek divorce based on one party's mental unsoundness which may necessitate a medical examination and the other party's privacy right. It held that it can order a medical examination if the individual presents a strong case.

National Legal Services Authority v. Union of India,[48] In this case, the court determined that the foundation of individuals identity, gender expression and gender appearance is because of gender identity and it must be safeguarded by the Art. 19(1)(a) of the constitution of India. Actions and physical appearance might reveal aspects of their personality of a transgender. The state cannot forbid, limit, or interfere with a transgender person's capacity to express their personality, which is a reflection of their fundamental nature. Because of ignorance or for other reasons, the State and its governing bodies sometimes fail to comprehend the fundamental essence and personality of such people. We thus contend that the basic rights to privacy, individual autonomy and pride that the transgender community members are protected by Article 19(1)(a) of the Indian Constitution which must be upheld and acknowledged by the state.[49]

2.6.2 RIGHTS OF WOMEN

The Supreme Court has emphasized that women right to privacy encompasses various aspects such as reproductive autonomy. This includes the freedom to use contraceptives and the right to undergo an abortion. Rape is a major infringement which is safeguarded by Article 21 of the Constitution, according to the Court, which has argued for harsh penalties for sexual assault.[50] A guideline has been issued to preserve the privacy and comfort of women who are witnesses or accused in situations of torture and harassment of women within police stations. According to the directive, female police officers must conduct interviews with these women at their residences thereby addressing the concerns raised and promoting a safer and more respectful environment for women involved in legal proceedings.[51] The Supreme Court deemed the

[47] AIR 2003 SC 3450
[48] (2014) 5 SCC 478
[49] Ibid
[50] State of Karnataka v. Krishnappa, (2000) 4 SCC 75
[51] State v. N.M.T. Joy Immaculate, (2004) 5 SCC 729

enforcement of conjugal rights as an extreme measure that infringed upon a woman autonomy over her own body. Because it violated her right to privacy, it was determined to be unlawful.[52]

State of Maharashtra v. Madhukar Narayan Mardikar,[53] the issue of prostitute's rights came to the forefront when a police officer was terminated due to his inappropriate conduct with a woman. The Maharashtra High Court doubting the credibility of the woman testimony concluded that her evidence was unreliable. However, the Supreme Court took a different stance and upheld the right to privacy for prostitute's emphasizing that violating their privacy cannot be justified by making assumptions about their moral character. According to the court, everyone is allowed to maintain their anonymity and has a basic right to privacy.

The Supreme Court was dealing a case related to a police officer who was accused of unlawfully entering the women residence while in uniform and sexually assaulting her. In their ruling, Justices K. Jagannatha Shetty and A.M. Ahmadi of the apex court upheld the right to privacy for prostitutes. It held that even a female with simple morals has a right to privacy, which no one is permitted to violate whenever desires. Furthermore, anyone who violates her won't be allowed to do so anytime they want. She has the right to protect herself if someone tries to enter her personal space against her consent. She is also having the right to be safeguarded under the law. Therefore, a women testimony cannot be overlooked since she possesses a straightforward nature. In order to examine her evidence, the officer would at most need to exercise care before accepting it.[54]

In *Roe v. Wade (1973),*[55] Right to privacy is safeguarded by the Fourteenth Amendment, according to the US Supreme Court, which allow woman to undergo abortion. In the case of *Suchita Srivastava v. Chandigarh Administration,*[56] The question pertained to the termination of a pregnancy involving a mentally challenged orphan woman who had been a victim of rape. There is no doubt that a woman is having the right to make their own reproductive decisions comes under the term of individual liberty as specified in Art. 21 of the constitution, it was decided. One must realise that they have the reproductive freedom to choose whether or not to have children. The need to defend a women privacy, reputation and self-determination should always be kept in mind. This shows that there shouldn't be any constraints on a woman capacity

[52] Saroj Rani v. Sudarshan Kumar Chadha, (1984) 4 SCC 90
[53] (1991) 1 SCC 57
[54] (1991) 1 SCC 57, Para 8
[55] 410 U.S. 113 (1973)
[56] (2009) 9 SCC 1

to exercise her reproductive choices such as her right to reject sexual activity or, on the other hand, the focus placed on utilising contraceptive methods.[57]

The expansion of the concept of privacy has resulted in a wider understanding that encompasses numerous instances of violations of women rights. In the present legal era, the right to privacy significantly influences the rights of women.

2.6.3 PROTECTION OF PERSONAL INFORMATION

We are currently in the age of abundant information facilitated by the internet which has made the world easily accessible to us. Our online activities such as transactions and website visits leave behind digital traces that are stored and recorded. These footprints hold details about individuals and their preferences. These seemingly unimportant individual traces reveal human characteristics including personality, food preferences, sexual orientation, health status, social connections, lifestyle, and political beliefs when they are combined.

In *NASA v. Nelson*[58], unanimously determined that the background checks conducted by NASA on contract employees did not infringe any private rights granted by the Constitution, allaying worries about issues relating to informational privacy. The court stated that given the safeguards outlined by the Privacy Act's concealment requirement and the reality that the portions of the forms under challenge consist of reasonable questions in an employment background check, we come to the conclusion that the Government's concerns do not violate a constitutional right to data privacy.

In *R v. The Commissioner of Police of the Metropolis,*[59] The extent of the police power to keep biometric information about people who are no longer suspected of committing a crime has been questioned in accordance with the standards established by the Association of Chief Police Officers (ACPO). The police practise of keeping DNA evidence without "extraordinary circumstances" is illegal and in violation of Article 8 of the European Convention on Human Rights, the UK Supreme Court found unanimously.

Due to the distinctive properties of information, maintaining privacy has grown more difficult in the information era. Information has three separate properties: recombinant, non-rivalrous,

[57] Ibid
[58] 562 U.S. 134, 131 S. Ct. 746 (2011)
[59] [2011] UKSC 21

and invisible.[60] It is exceedingly difficult for a judge to imagine every potential uses for data or predict the consequences in the age of growing technology.

Privacy laws regarding data get more complicated as more technology emerges as it includes data that a person had no access to and failed to disclose, either intentionally or unintentionally. Furthermore, the nation has been called an "information state" which is seen to be the origin of all social, economic and political issues decisions as a result of its rising dependence on information. This becomes difficult to keep track of all the probable issues related to the use of information. The courts in such a circumstance face a difficult task since they are required to foresee and address invisible, developing damages.[61]

As the current era is characterised by a complex and delicate balance that must be struck between the legitimate concerns of the state and the individual's right to privacy protection, dataveillance or the systematic use of information technology to monitor citizen communications or behaviours, is increasingly common.[62] This balance gives rise to intricate challenges requiring careful considerations and the establishment of harmonious relationships between these two aspects.

2.7 CONCLUSION

The ability to live with dignity depends on the exercise of a complicated and inalienable right to privacy. As society has developed over time, so the understanding of privacy as a basic right is essential. The right to privacy is inherent under constitution including Article 21. It is crucial to remember that the right to privacy is not absolute. An absolute right to privacy poses threats to law, order, and security, and it is also practically impossible. An individual privacy can be invaded only by the state in accordance with the law, for valid reasons, and in a fair way.

[60] Christina P. Moniodis, Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy, 15:1Yale Journal of Law and Technology 154, (2012)
[61] Ibid
[62] Yvonne McDermott, Conceptualizing the right to data protection in an era of Big Data, Big Data and Society 1, (2017)

CHAPTER-3

3. UNDERSTANDING DATA PRIVACY INCLUDING THE RIGHT TO ERASURE AND RIGHT TO BE FORGOTTEN

3.1 INTRODUCTION

In today's digital era, where we heavily rely on various digital tools for almost every aspect of our daily lives, we often overlook the fact that we are constantly leaving behind permanent digital traces. Daniel J. Solove, in his book titled "The Digital Person,"[63] sheds light on the invasion of privacy and the everlasting storage of data in this information age. Solove explains how our personal information is constantly being compromised and how it is retained indefinitely in the digital realm. According to one experts, there will come a day when we will be widely recognised for our inclinations, predilections, proclivities and desires. We shall be classed, profiled, and categorised, and every click we make will be recorded. Despite the growing amount of time that we engage online, we are developing an indelible record that is more detailed and widespread than any other record. In reality, most internet-based content is being recorded. One corporation has even been cautiously collecting every piece of information from the Internet and keeping it in a massive computerised storehouse.[64] Our digital personas are expressed through the content we share on websites and social media platforms. We have grown accustomed to the transient nature of online material with things appearing and disappearing giving us the impression of impermanence. However, very little is actually lost or forgotten when we edit or remove anything on the internet. As we human beings increasingly migrate into the digital realm, the amount of information stored online will only continue to grow.[65]

3.2 DATA AND BIG DATA

Data refers to documented information or patterns that convey observations, actions or symbolic representations of values or activities observed. Examples include readings from

[63] Daniel J Solove, The Digital Person, 26 (New York University Press, 2004).
[64] Ibid
[65] Ibid

instruments, x-ray or scanner images, recorded voices, family lineage charts, interview answers, medical billing records and numerous other outcomes resulting from processes like observation, inquiry, listening, measurement, documentation or analysis.[66] Most research data is now handled in digital formats even if it requires converting from non-digital sources. This has significant advantages such as facilitating computerized analysis and allowing quick and cost effective data transmission between locations. However, the way data is managed and utilized determines whether these advancements are beneficial or problematic. The term "information" pertains to data that has been contextualized to derive meaning and it is often used interchangeably with the term "data."[67]

Data is defined in Sec 2(4) of the draft of Digital Personal Data Protection Bill, 2022 as Data refers to a representation of facts, ideas, views or instructions that is appropriate for human or automated interpretation, transmission or processing.[68] "personal data"- implies any information about a person that may be used to identify them.[69]

Data is a standardised representation of the information that is currently being handled or previously processed by an electronic device or computer system network. It might be information, details, ideas, or commands. Data can be kept electronically in the memory of the computer or it can appear in any format, such as digital printouts.

According to International Business Machines Corporation, like philosophy is not about words, neither is big data about the data. Big Data focuses on the significance which is able to be extracted from the information or the possible importance of the information. The term "Big Data" signifies the procedure of the extraction process which indicates that more information is being generated at greater speeds from various sources and in various forms than at any time. We ought to definitely replace big data to big meaning since big data is really about the significance in the information, not the information itself.

The concept of the Internet of Things (IoT) involves incorporating sensors and mechanisms into ordinary objects like refrigerators, cars (especially self-driving ones), roads, pacemakers and watches. These sensors collect and store data, which can be transmitted wirelessly to other

[66] William W. Lowrance, Privacy, Confidentiality And Health Research 7 (Cambridge University Press, 2012).
[67] Ibid
[68] Sec 2(4) of the draft of Digital Personal Data Protection Bill, 2022.
[69] Sec 2(13) of the draft of Digital Personal Data Protection Bill, 2022.

objects or machines via the Internet. The accumulation of this data is commonly referred to as "big data."

In a report submitted to the White House[70], the term "IoT" was defined as:

The capacity of devices to connect with one another via embedded sensors coupled via wired and wireless networks is referred to as networking. These appliances may be your vehicle, the temperature regulator, or the medicine you take which allows your physician to monitor the health of your digestive system. These internet connected gadgets send, gather and process data via the internet.

The range and complexity of data sources and formats are expanding rapidly. This encompasses various examples such as the internet, social media platforms, mobile apps, government databases at the federal, state and local levels, commercial datasets that aggregate personal information from numerous commercial activities and citizen information, specificied geographical location data, survey and conventional data that were converted to digital format through scanning. The increasing availability of Internet-connected devices and sensors has broadened the scope of collecting data from physical objects like detectors and radio-frequency identification (RFID) chips. It is now possible to gather personal location data through various means such as GPS devices, triangulation of cell towers, mapping wireless networks and transactions made in person.

Every day, the activities of billions of individuals using electronic devices such as computers and mobile phones result in the creation and collection of massive volumes of data. This includes online financial transactions, social media interactions, and global positioning system coordinates. Big data enables access to information about individuals that was previously impossible to obtain in past generations. By collecting and integrating vast datasets, it unveils details such as a person's communication networks, conversations, locations visited, workplace, connections with family and friends, dining preferences, purchasing habits, and more. It also provides details into their personal preferences, hobbies, financial and employment statuses and even any past criminal records. This comprehensive data allows for the creation of complete profiles of individuals.

[70] Big Data: Seizing Opportunities and Preserving Values, Executive Office of the President, May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf accessed on 30/05/23

3.3 THE IMPACT OF THE DIGITAL AGE ON PRIVACY

In the context of network societies, individuals have simultaneously taken on the roles of data subjects and quantified self. The quantified self concept relies on the collection of large amounts of data through various mechanisms which not only involves individuals willingly engaging with measurement and computing technologies but also actively participating in the process of quantification. In doing so, individuals become active agents within the technological systems that interact with their bodies. Simultaneously, the notion of the data subject is closely connected to the quantified self but specifically focuses on how individuals express themselves establish their identities, experience subjectivity and navigate the networked technologies that shape various aspects of their lives, work and communication.[71]

Technology has become an essential part of our daily lives connecting us to the world around us. Our shopping habits have shifted from local stores to online purchases and we now rely on the internet to buy groceries, book travel accommodations and even purchase medicine. The availability of e-books has greatly expanded our access to knowledge and online banking has made financial transactions more convenient often accompanied by special offers and cashback incentives. The internet is now a versatile tool used for communication, commerce and various other activities. Whenever we have questions, we turn to search engines like Google for instant answers.

Despite the numerous advantages offered by the internet, its effect on an individual's privacy is frequently overlooked. Each website we visit and each transaction we conduct leaves digital traces, frequently without our knowledge. These digital footprints hold information that can reveal details about the user. While these individual pieces of information may appear insignificant, when combined, they expose aspects such as personality, dietary preferences, language usage, health status, hobbies, fashion choices, social and familial connections, political affiliations and religious beliefs.

Websites commonly use cookies to store information in a user's browser enabling quick recognition and the safeguarding of online activity data. User profiles are built using this information, particularly their browsing history. Algorithms are employed to create these profiles on the internet. Automated content analysis of emails allows for the extraction of

[71] Nishant Shah, Identity and Identification: The Individual in the Time of Networked Governance, 11 Socio-LEGAL REV. 22 (2015).

relevant information and interests which can then be used to target appropriate advertisements to users on the website. Online purchases such as books leave a trace that can be utilized for targeted advertising within the same category. Details like whether a flight ticket was bought in economy or business class can provide insights into a person's work status and economic capacity. Online cab bookings to shopping malls aid in creating a profile of client preferences. For instance, a lady who makes an internet purchase of pregnancy-related medications can start getting adverts for baby products. Overall, electronic surveillance of people's lives has become widespread.

In the case of *Whalen v. Roe,*[72] the Supreme Court of the US acknowledged its understanding of the privacy concerns associated with information technology, stating:

We recognise the potential danger to security that comes from the gathering of huge quantities of private information in electronic information stores or other major government information systems. Massive amounts of data, the majority of which are sensitive and could be demoralising or dangerous if shared, must be preserved in a systematic manner in order for taxes to be collected, welfare and social security benefits to be paid out, public health to be regulated, our armed forces to be run, and criminal laws to be administered.

In his explanation, Daniel Solove highlights the potential threat to privacy when seemingly harmless pieces of information are combined creating a comprehensive and intricate depiction of our personalities and actions. This combination of data pieces unveils a detailed profile that poses risks to our privacy. Solove refers to the issue as "aggregation" and highlights how businesses and governments frequently combine diverse fragments of information even those that may not be considered private on their own in order to create a comprehensive profile or image.

He explains, as noted by law scholar Julie Cohen, An in-depth examination of information provided by an individual is significantly greater then the entirety of its components. I call this occurrence the "aggregation effect". Similarly to the way a Seurat's picture is created where several lines are put together against one another to generate an image, data may be utilised to create a picture of an individual. Personal data is being merged in the Information Age to generate a digital biography about ourselves. Frequently seemingly inconsequential details become important to more private information keeping facilities or serves as an essential part

[72] 429 U.S. 589 (1977).

of an individual's electronic biography. Stan Karas, a specialist in law, argues that the items we consume are a reflection of who we are.

In her article, Christian P. Moniodis[73] highlights, the distinctive elements associated with data that poses challenges in identifying breaches of privacy. Since information is nonrivalrous, invisible, and recombinant in nature, it has a complexity that is fundamental to information privacy. In matters involving data privacy, these characteristics render courts almost oblivious to the harms involved. First of all, information may be used by several people at once, making it a nonrival good. This means that the process of use of any data by a particular individual has no impact on other users ability to access it. Private information attacks may also be unnoticed, rendering it challenging to identify. Data may be examined, preserved and transmitted without prior notification. Accessing data is more challenging to identify as data could travel at the velocity of light, allowing obtaining data the most rapid kind of fraud. Thus, in addition to independent use of data, large violations of privacy are possible without noticeably affecting those whose confidentiality has been breached. Furthermore, as details are recombinant, information produced may be exploited as a source for generating more data results and so on. As an example, an innovative tool known as discovery of information as well as data mining methods can possibly be utilised in order to "develop facts" regarding an individual using data, particularly to predict that a person is going to participate in a specific kind of action. Privacy laws concerning data have more complex as improved understanding emerges because it includes details that a person had no access to or failed to make public, either knowingly or involuntarily. Furthermore, as our society progresses into a "knowledge state" using an increasing dependence on data, that has been referred to as the bloodstream that underpins governance, society, and economic choices, it is relentlessly to predict any of the prospective usage of data and the associated problems. A problem emerges when courts are necessary to prepare for and solve undetectable, developing adverse effects.

Advancements in technology have simplified the acquisition of images that were previously challenging for the general public to obtain. This has been made possible by covert "soft surveillance" methods and the creation of new sensory-expanding technology, making data that was previously unavailable available. However, the concerning aspect of such surveillance is that it allows for the gathering of private data without their authorization or permission of the

[73] Christina P. Moniodis, Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy, 15:1Yale Journal of Law and Technology 154, (2012)

individuals involved, thus creating possibilities for misuse in order to provide the necessary customisation, the expanding business models, which place a growing emphasis on customising services and goods to individual interests, call for the collecting of vast amounts of personal data.

3.3.1 THE ADVERSE EFFECTS OF COLLECTING PERSONAL DATA

The adverse effects of collecting personal data are discussed by Moira Paterson & Maeve McDonagh.[74]

Big Personal Data undermines individual freedom and is therefore damaging to privacy since it prevents people from exercising authority over their own private information. Liberal thought is based on the idea of autonomy. According to Christman, the concept of individual autonomy is commonly believed to relate to the capacity to be able to life for an individual in accordance with the purpose and objectives that are seen as the individuals and not as a conclusion of distortive or manipulative outer factors, Big Personal Data weakens the freedom of information subjects in clarification of their information, unless it is solely based on evaluation of data collected and used with the consent and knowledge of the individuals concerned; this also promotes actions and behaviours which further weaken independence by subjecting their choices to manipulation.

It undermines the value and worth of individuals by disregarding their preferences in respect of using an individuals private information and neglecting their feelings about how their data is handled. Additionally, it reduces human dignity by treating people as mere objects of analysis and enabling decision making processes that further dehumanize them.

The collection of personal data can provide valuable insights into people's behavior, vulnerabilities and other aspects which can potentially be exploited to manipulate them. One instance of such exploitation is evident in political campaigns where accusations have been made about the utilization of analytics to sway the results of the Brexit referendum and the 2016 US presidential elections. Cathy O'Neil contends that the practice of data profiling is increasingly prevalent in the realm of politics. Political campaigns are developing scoring systems to assess potential voters, determining their probability of supporting a particular party,

[74] Moira Paterson & Maeve McDonagh, Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data, 44 Monash University Law Review 1 (2018).

their position on specific issues and their susceptibility to persuasion on those issues.[75] This imbalance of information is then utilized by politicians to influence individual's voting decisions or donations.

For example, WalMart in the United States utilizes a combination of sales, pricing and economic information along with demographic and weather data to optimize its merchandising strategies and predict the optimal timing for store sales. Big Personal Data-based making decisions also subjects individuals and organisations to unequal treatment (for instance, pricing discrimination based on various discounts). This is discrimination since it enables the creation of subtle differences between people which are subsequently utilised as the foundation for unequal treatment. While these procedures are standard in some industries, such as the insurance industry, big personal data enables their more broad use in regard to information that was not previously accessible. This raises crucial considerations about whether there are "specific differences" that go beyond those already covered by anti-discrimination rules and should not be disregarded.

In the present era, corporations have a strong desire to acquire as much customer data as possible and their pursuit of information is far from equitable. The data, they collect extends beyond consumers opinions of their products and encompasses personal aspects of the consumers including lifestyle information and even a thorough psychological profile.

3.3.2 STATE'S PROCESS OF GATHERING INFORMATION: DATA COLLECTION

The 9/11 terrorist attack in the United States led to a widespread demand for enhanced national security measures. This event played a significant role in normalizing the use of state surveillance as a means of ensuring the safety and security of nations worldwide. Edward Snowden's revelations in 2013 brought to light that the United States National Security Agency had been monitoring the phone conversations of its own citizens.

In his article 'Privacy, Surveillance and Law' Richard A. Posner discusses that state led data surveillance can play a crucial role in safeguarding national security. According to Posner, if individual profiles are converted into digital format, combined and electronically searched, it would uncover connections and interactions between people. This wealth of information would

[75] Cathy O Neil, Big Data Algorithms are Manipulating Us, WIRED, https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/- accessed on 30-05-2023

prove invaluable for intelligence agencies in identifying and monitoring members of terrorist organizations as well as uncovering their networks and sources of funding. He debated that The internet, with its secure encryption and anonymity of digitised information that, if merged with that confidentiality, make the internet an influential tool of conspiracy, has enhanced the privacy of terrorists, who have benefited from the same advancements of technologies which have been made data mining achievable and extract countless amounts of private data from innocents. To protect national security, government has an urgent need to use digitalization.

In *Osborn v. United States,*[76] Justice William O. Douglas expressed his dissenting opinion. There may come a time when no one knows if what they say is being recorded for use at a later date; when everyone will be afraid that his most private opinions are no longer his own but instead belong to the government; and when even the most private and personal discussions are always accessible to eager, surveillance ears. When that day arrives, liberty and privacy will both be lost. Who can claim that an individual is free if his privacy can be violated at any time? Who can claim to enjoy freedom of expression if every word he says is recorded and scrutinised or if he is scared it could be? Who can claim that someone has the right to freedom of association if every association they make is recognised and documented and if their interactions with other people are stolen? When such circumstances exist, people like us will be hesitant to speak anything but the safest, most conventional opinions and to associate with anybody but the ones who are most deserving of their approval. The Constitution's vision of freedom will no longer exist.

In regard to national security concerns, the government has other motive for gathering and retaining data. The collection of data is necessary for effective administration, including the fair allocation of resources, crime management, and appropriate distribution of funds. By analysing this data, it becomes possible to validate rightful claims and prevent the misappropriation of resources by unauthorized individuals. In a welfare oriented society, the collection, storage and analysis of data are essential for the smooth operation of the state.

[76] 385 U.S. 323 (1966)

3.3.3 DATAVEILLANCE

In the realm of cyberspace, the process of gathering information generates highly specific and easily manipulatable data which is tied to individuals and remains accessible indefinitely. This combination is further enhanced by the significantly reduced cost of collecting and analysing data in cyberspace compared to the physical world.

According to information technology expert Roger Clarke, the term “dataveillance” pertains to the organized utilization of personal data systems to examine or observe the activities or communications of individuals or groups. According to Colin Bennett, the concept of dataveillance refers to the surveillance methods enabled by the extensive gathering and retention of large volumes of personal information. Dataveillance represents an approach to monitor individuals distinct from traditional means of observation such as visual or camera based surveillance. Instead, it relies on the accumulation and analysis of factual details and data. Surveillance represents a violation of human dignity as it infringes upon one's ability to freely choose, resulting in a form of self-censorship. Increasing data collection has the potential to restrict one’s ability to make free choices as more information is gathered about an individual, it becomes simpler to manipulate them into compliance. Databases pose a challenge as they can function as a means of surveillance that restricts personal liberty.

Dataveillance can be considered as the contemporary adaptation of Jeremy Bentham’s concept of the ‘panopticon.’ In the panopticon, a circular prison design allowed for constant surveillance of prisoners who remained unaware of when they were being observed. Similarly, dataveillance involves the monitoring and scrutiny of individuals through the collection and analysis of their digital data. This modern version of surveillance operates subtly and covertly creating a pervasive sense of observation without the knowledge of those being watched.

George Orwell’s (1984) said that “Big brother is watching you”. Orwell noted that television cameras and microphones to be present day surveillance tools. However, the digital computer, of which Orwell was unaware, is a much more powerful monitoring tool that can be used for this purpose by both the public and private sectors. According to Adam De Moore, surveillance techniques for law enforcement agencies might include video monitoring, global positioning systems, biometric technology and data collection without unnecessarily burdening people who are being monitored.

In *United States v. Jones,*[77] According to Justice Sonia Sotomayor, new monitoring techniques do not need physical searches or intrusions. It was held that GPS tracking creates an accurate, detailed record of a person's public travels that contains an abundance of information about her sexual orientation and political, professional and social affiliations. The government may safeguard these types of records and easily analyse them for information throughout years to come. Furthermore, since GPS tracking is less expensive than traditional surveillance methods and operates covertly by design, it avoids the usual constraints that restrict oppressive law enforcement practises, such as a lack of police resources and opposition from the community. The installation of GPS was determined absolutely unanimously, it is a device to monitor the movement of a car or track any sort of vehicles travelling involves a fourth amendment search.

3.4 PRIVACY OF DATA

Digital privacy refers to the control one has over how their online identity is created and how and with whom they choose to disclose particular aspects of it. Conceptually, privacy is the freedom to establish one's own identity online. Privacy is the capacity to create and maintain a digital self-portrait that represents one's own preferences.

In the book, "Digital Data Collection and Information Privacy Law" written by Mark Burdon emphasizes data privacy law. The legislation governing information privacy gives a number of life cycle safeguards that start at the time of obtaining individual information and finish with the deletion of data that is no further needed. In meantime, collecting information organisations have to keep to a number of requirements. For example, the person must be informed of the intent of collection so they can effectively agree to future uses. In general, private information can be used for a particular reason that the subject has been properly made aware of. People may confirm the correctness and relevance of the personal information that has been obtained using a variety of engagement methods that aim to assure the maintenance of control. Once gathered and stored, personal data needs to be kept safe.

The institution gathering the data is expected to use fair information practices while gathering personal information. Organization's that collect and use personal information must pay attention to fair information practices which are code of conduct in order to guarantee that the

[77] 565 US 400 (2012)

data is properly safeguarded. These procedures include notifying individuals who have personal information about the collection of their information, providing them with choices regarding the use of their information, enabling individuals to review and contest information pertaining to them in a timely and cost-efficient manner, and taking steps to ensure that the data acquired concerning them is correct.

The US FTC has advocated for federal legislation requiring the application of the four principles of fair information practice--notice, choice, access, and security--to commercial Web sites. These principles were initially created due to concern over the effect on people's privacy of the rapid development of computerised records between a host of government organisations. The principle of notice, when used to an online context, mandates that commercial websites disclose to their users what personally identifiable data about them is being collected, how it is being collected, whether it will be shared with other organisations, and whether other parties are allowed to collect details at these websites. Websites should allow the online users to choose whether the data they willingly give them for another purpose in order to provide them an appropriate level of choice. The access principle allows users to see the information that has been gathered concerning them by a specific website and make any required modifications, but the security principle mandates that Web sites keep the private information that they collect from being accessed by unauthorised parties.

3.5 RIGHT TO BE FORGOTTEN

The story of one Ms. Stacy Snyder is told at the beginning of the book, "Delete"[78]. Ms. Stacy, a 25 year old single mother, has all the qualifications needed to get recruited as a teacher. The university summoned her to notify her that she had been refused the certificate because her actions was 'unbecoming' of a teacher. It was somewhat unexpected to know the justification behind the university's decision. The incident in question was a photograph she uploaded on the social media site "MySpace" in which she was dressed like a pirate, holding a plastic cup and drinking from it with the caption "drunken pirate." She made an attempt to delete the picture following this occurrence. Unfortunately, the harm had already been done. However, what Stacy intended to delete, forget and wipe from the Internet was remembered.

[78] Viktor Mayer Schonberger, Delete: The Virtue Of Forgetting In The Digital Age, (Princeton University Press, 2009)

The type and volume of information that is available on people has changed substantially since the development of the Internet. The only sources of personal data are no longer newspaper articles and official documents or government records. Every website or activity we like or share along with our online social networking, Tweets, photos and videos we post or in which we are mentioned and every website or event we bookmark, like or share contributes to our digital footprint. It is plainly clear that we are living in a Big Data world where computers monitor the repetitious activity of our digital lives. A technique that enables part of this digital shadow to be erased makes sense in this situation.[79]

3.5.1 GOOGLE SPAIN CASE[80]

One Mr. Gonsalez made a request to the Spanish Data Protection Agency asking for the deletion of search results that his name on Google. The results were newspaper articles about a long ago auction held to pay off his debts. Mr. Gonzalez stated that any references to the processes in question were no longer relevant because of the passage of time and the fact that they were completed. While Google's complaint was upheld, the Spanish Data Protection Agency discontinued its lawsuit against the publication. The information was mandated to be blocked from future access and deleted from Google's index. Google submitted a petition asking for the judgement to be reversed. Back the the Court of Justice of the EU was sent a number of enquiries by the Spanish Court.

The court determined that Google "processed" private information since it made possible for any internet user to enter a structured abstract information pertaining to that person online by doing a name search. With the help of search engine Mr. Gonzalez's private life was revealed connected with the information which were not possible to be found. Hence search engines increase the interruption of individual privacy by making data "ubiquitous" and it worsen the breach of one's privacy, the court stated. The operator of the search engine's simple economic interest could not provide sufficient justification for the potentially very serious rights violations. The most significant finding of the court was that even data processing that is currently legal might eventually become illegal. This could be the situation if the information are not maintained or held for a long period of time for the purpose it was collected. They may

[79] Amber Sinha, Right to be Forgotten – A Tale of two Judgments, Centre for Internet Society, accessed on 09/06/23 https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-juSdgments
[80] Google Spain SL, Google Inc v. Agencia Espanola de Proteccion de Datos es Mario Costeja Gonzalez ECLI:EU:C:2014:317 [Case Number C-131/12]

also be insufficient, irrelevant or excessive in relation to the processing's objectives. The court reached the conclusion that in the majority of cases the privacy rights guaranteed by the European Charter should take precedence over both the corporate interests of the search engine operator and also the interests of the common people.

The right to be forgotten represents an individual's demand to have certain information erased so as the third parties won't be able to recognise them. It is defined as having the right to maintain silence about things that have already occurred but are no longer occurring,[81] public request to private information, videos or photographs be taken down from particular internet records so that they do not show up in search results pages are enabled by the right to be forgotten. In contradiction to the right to be forgotten which entails erasing previously available material and preventing access to it, the right to privacy refers to information that is not publicly accessible.[82]

The right to be forgotten, in principle, resolves an important issue in the digital era when it is highly challenging to erase one's online past due to the fact that every tweet, status update, and photo is now permanently kept in the cloud. Europeans and Americans, however, address the issue very differently. The legal basis for the concept of the right to be forgotten in Europe can be found in French law which recognises the "right of oblivion", or le droit I l'oubli, which entitles a convicted felon who has completed his sentence to object to the expose of data about his sentence and imprisonment for the purpose of reintegration into society.

'Delete; The virtue of forgetting in the Digital Age' describes a distressing historic instance of the misuse of data obtained.[83] The Dutch government established a population register in the 1930s to gather details about its resident's name, address, date of birth, religion and other information. In order to make administration and policymaking easier, the register was established. However, the registration was taken over by the Nazis when they conquered the Netherlands. The information was used to track down and brutally persecute Jews. The register made it simple for the Nazis to identify Jews and thus the Netherlands saw the greatest rate of

[81] Pino, G. (2000). "The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights". In: M. Van Hoecke; F. Ost (eds.). The harmonization of private law in Europe (pp. 225-237). Oxford: Hart Publishing. p. 237.

[82] Kashmir Hill, (July 6, 2011). "Revenge Porn With A Facebook Twist". Forbes. Accessed on 09/06/2023, https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=4393773b1d2e

[83] Viktor Mayer Schonberger, Delete: The Virtue Of Forgetting In The Digital Age, 85 (Princeton University Press, 2009)

persecution. The author claims that the people trusted their government and had no clue what the future held for them and he issues a warning that this might happen to any nation.

3.5.2 RIGHT TO BE FORGOTTEN ACROSS THE GLOBE

- **EUROPEAN UNION**

The right to be forgotten is a concept outlined in the 1995 European Union Data Protection Directive. According to Article 12 of the Directive, if the data is no longer required, a person may request that it be corrected, removed or blocked. The EU's right to be forgotten has also been affirmed by the Google Spain case. In accordance with Article 17 of the EU Regulation 2016, individuals have the right to ask that their private data be deleted in which doing so becomes necessary to comply with Union or Member State laws to which the data controller is subject. It additionally is applicable in cases where the private data is no longer needed for the reasons which it was gathered or otherwise processed.

- **UNITED STATES**

About a year after the Costeja decision, in June 2015, Google made an important change to its user guideline regarding deleting links from Google searches. Particularly for victims of revenge porn, the change was applicable to persons in the US and other countries. Revenge porn is when someone posts naked images of an ex-lover on the internet. When Google searches for their identities turn up naked images of them, female revenge porn victims have described terrifying ordeals. The policy change signalled a significant shift in Google's strategy. Except for a restricted category of personal information such as signatures, bank accounts and other sensitive ID information, Google has been mostly unresponsive to user requests for privacy related changes to search results. Google will permit the removal of a link from search results under certain specific conditions. Moreover, google has made it possible to derank websites that have received repeated copyright infringement notifications as well as

search results that include images of individuals in jail.[84] This demonstrates how the US is increasingly enforcing the right to be forgotten.

3.5.3 RIGHT TO BE FORGOTTEN IN INDIA

When it comes to privacy, the right to be forgotten is covered. In India, the right to be forgotten raises difficult legal issues. The Information Technology (IT) Act 2000 (as amended in 2008) and the IT Rules, 2011 in India do not have such a clause, despite the significance of such a right. Various High Courts have expressed divergent opinions.

- *Dharamraj Bhanushankar Dave v. State of Gujarat & Ors*[85]

An appeal was filed against the Gujarat High Court's publishing of an Indian Kanoon decision that Google had listed as a "non-reportable judgement" in its search results. It was a violation of Article 21 in the petitioner's opinion. The petitioner argued that Google and Indian Kanoon lacked legal authority to publish a non-reportable decision which had impacted his personal and professional life. He also argued that the judgement was widely accessible online as a result of the revelation, contradicting the Court's categorisation.

The Court observed that the term reportable is used for judgement in regard to it being published in law reporters, therefore just publishing the judgement in the appeal on the internet would not constitute reporting it. The judgement in the appeal constitutes an element of the processes and the stated judgement is delivered by this Court.[86]

According to the Court, there was no legal justification for such a removal order and the petitioner's Article 21 rights were not violated by the judgment's availability online.

[84] Edward Lee, "The Right to be Forgotten v. Free Speech" Journal of Law and Policy for the Information Society, 103 (2015)
[85] 2017 SCC Online Guj 2493
[86] Id

- *Sri Vasunathan v. The Registrar General*[87]

As his daughter feared the repercussions of having her name connected to this earlier matter, the petitioner, a father, filed a Writ Petition in the Karnataka High Court asking for orders to block his daughter's name in an earlier order passed by the Court. If a name-wise search was performed by anyone through any internet service provider such as Google or Yahoo, these results could include this order. The daughter of the petitioners was worried that this would ruin her marriage as well as her reputation and societal standing.

The Court observed that this would be in accordance with the "right to be forgotten" concept in western countries in critical instances including women in general and in particularly delicate circumstances involving rape or harming the dignity and image of the person involved.

The Court directed the registrar to use all reasonable efforts to ensure that any public domain internet search does not show up the name of the petitioner's daughter in the case title or the details of the order in the criminal petition.

- *Judgement of the Kerala High Court in the Civil Writ Petition No. 9478 of 2016*

The Kerala High Court ruled in support of the Right to be forgotten in a decision dated February 23, 2017. In this instance, the petitioner approached the Kerala High Court with a writ petition to protect their right to privacy under Article 21 of the Constitution. The petitioner requested the court to grant directions assuring that their identity would be secured and that any things including their name on Indian Kanoon, Yahoo and Google would be erased or properly disguised. Considering the importance of the matter and Indian Kanoon's failure to appear in court regardless of being served with a notice, the Court issued an interim order in the petitioner's favour ordering Indian Kanoon to remove the petitioner's name from orders posted on its website until further orders had been issued.

- *Zulfiqar Ahman Khan v. M/s Quintillion*[88]

Following the #metoo campaign, the petitioner sought the Delhi High Court to order the defendants to remove the news that had published against him. Taking into account the

[87] 2017 SCC Online Kar 424
[88] 2019 SCC Online Del 8494

Plaintiff's right to privacy which includes the Right to be Forgotten and Right to be Left Alone, the court issued an order: Any republishing of the original material of the disputed articles from October 12 and October 31 or any excerpts or modified versions of those instances on any kind of publication or digital/electronic media must be prohibited while the current lawsuit is pending.

- *Subhranshu Rout v. State of Orissa*[89]

The accused who committed a rape on a lady and posted a video of it online/social media filed a bail application with the Orissa High Court. The court denied him bail while taking into account the right to be forgotten and held, Without a woman authorization, permitting such offensive images and videos to stay on a social networking site is an outright violation of the modesty of a woman and, more significantly, her freedom of privacy. In such circumstances, either the victim or the prosecution may, if notified, obtain suitable steps that safeguard the victim's basic rights regarding privacy by requesting that such offensive content be removed from an open platform, regardless of the current criminal procedure.[90]

- *Karthick Theodore v. Madras High Court*[91]

The Madras High Court rejected a request in regard to the identity of the accused who had been acquitted of all charges, be deleted from the court orders. The Court observed, This Court really believes that the criminal justice system in our country has not yet reached the point where judges may dare to order the removal of an accused person's name based on specific objective requirements established by laws or regulations. To deal with the argument for removing the names of accused people who are found not guilty from criminal proceedings, it will be more suitable to wait for the implementation of the Data Protection Act and Regulations thereunder. These regulations may offer an objective standard. If such consistent norms are not upheld nationwide, the constitutional courts would be forced to ride a restless horse, which will be detrimental to the current system.

[89] 2020 SCC Online Ori 878
[90] Id
[91] 2021 SCC Online Mad 2755

- *Jorawer Singh Mundy v. Union of India and Others*[92]

The petitioner once had a case filed against him under the Narcotic Drugs and Psychotropic Substances Act of 1985 but he was eventually cleared of all allegations. However, an internet search of his name revealed criticism of the same which was damaging to his employment prospects. Until the final hearing, the Delhi High Court ordered Indian Kanoon to prevent the judgement from surfacing on search engines. The Supreme Court made the following observations in the Puttaswamy case[93] concerning the right to be forgotten, the "right to be forgotten" has been recognised by the 2016 European Union Regulation. This does not imply that every facet of former existence should be forgotten because some of them could have societal repercussions. A court were to come up with such a right, it simply means that an individual who no more needs his private data to be kept or assessed should be entitled to have it erased from the computer system if it is incorrect no longer relevant, or has no beneficial purpose at all. While data or particulars are necessary for the development, exercise, or defence of lawful rights, for the successful completion of an obligation executed out in the public's best interests in accordance with the requirements of people in general in the field of good health, for the storage reasons for academic or historical research purposes, for statistical examination, or for the use a different right, the right in question is inapplicable. In any instance involving privacy violation, notably data security violations, these justifications would be allowed.

3.6 RIGHT TO ERASURE

In the majority of legal systems, the terms "right to erasure" and "right to be forgotten" are interchangeable. The right to erasure commonly known as the right to be forgotten is covered in Article 17 of the GDPR. Furthermore, the "right to correction and erasure of personal data" is mentioned in Section 13 of the Digital Personal Data Protection Bill, 2022. It states:

(1) In accordance with the laws in force as well as the manner that might be monitored, an Information Principal has the right to request the rectification and removal of his/her own private data.

[92] 2021 SCC Online Del 2306
[93] (2017) 10 SCC 1

(2) After obtaining such an appeal from an information principal, the data fiduciary must respond to:

(a) erase the Data Principal's incorrect or deceptive private information;

(b) make a daata entry lacking private data about the data principal;

(c) to update the data principal imformation;

(d) Remove private information of an Information Principal which is not anymore needed for the reason that the data was analysed provided lawful storage is essential.[94]

3.7 CONCLUSION

We are now more dependent on the internet and the services it provides as a result of the development of the digital era. Despite the fact that we have successfully adapted to technology in many situations, it won't be prudent if we fail to acknowledge the shift to an electronic way of life.[95] Most of the time, we are not aware that our data is being gathered. For human dignity and personal liberty, data privacy is important. Despite the organisations are either private or public, individuals have the right to be aware how the data that is acquired is utilised. The permanent storage of information is not appropriate for a society which is growing. Citing Friedrich Nietzsche: "Without forgetting it is quite impossible to live at all". In order to build a brighter future, certain things must be forgotten, while others must be kept in mind. This privilege protects data from being transmitted into digital oblivion to some extent. In a time when each tweet, update or post may become part of the permanent internet, anybody who wants to delete any offensive information about them has the legal right to do so. The material must be kept up to date, however, for the benefit of the public. The right to privacy must be safeguarded without harming society peace, harmony or security.

[94] Section 13 of Digital Personal Data Potection Bill, 2022
[95] Arthur R. Miller, The Assault On Privacy, 39 (Ann Arbour, Michigan University Press, 1971)

CHAPTER-4

4. COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS

4.1 INTRODUCTION

Data security has become essential due to the rapid increase in digitalization across the world. Governments all across the globe are now more concerned with protecting rights of citizens than with regulating the internet. In spite of the fact that most developing nations like India are yet in the initial stages of developing laws, most developed nations involving the UK and the US have already raised the standard in this regard. The UK's 2018 Data Protection Act has its origins in the EU GDPR, while the US has a number of state laws as well as sectoral legislation to safeguard privacy.

4.2 THE PRIVACY AND SECURITY OF DATA IN THE UNITED STATES

In terms of data protection laws, the US takes a sectoral approach. No comprehensive federal legislation governing data protection exists. Instead, the federal legislation safeguards data in places that are relevant to particular sectors. Only certain area such as medical sector, educational sector, communication and financial assistance as well as minors in the instance of information collection are covered by these laws. On the other hand, most privacy regulations in the US place restrictions on how data are processed depending on the industry they are used in say, healthcare, banking, or education. In essence, privacy regulation in the United States is heavily dependent on privacy law or explicit consensus that are afterwards imposed by federal or state legislation. It is also highly sectoral, based in common law, and governed by both federal and state laws. Federal legal enforcement is administered by the FTC but state administration has always played a vital role in safeguarding customer's privacy. The US department of education, health and welfare's[96] advisory board first outlined the Fair Information Practise Principles in 1973, and they were later incorporated into the US Privacy Act of 1974. The Fair Information Practise Principles are a set of universally acknowledge

[96] Sec'y Advisory Comm. On Automated Personal Data Sys., U.S. Dept. of Health, Educ.&Welfare, Records, Computers and the Rights of Citizens (1973) https://aspe.hhs.gov/report/records-computers-and-rights-citizens accessed on 14/06/23

standards that have been used as the foundation for numerous privacy and information security legislation including those in the US, the EU and other countries.

4.2.1 FOURTH AMENDMENT

The US constitution fourth amendment specifies the limitation of US citizens privacy rights. It safeguards people from arbitrary government searches and seizures. In Katz v. United States, The Court found that the authoritie's unlawful surveillance of a person having a telephonic conversation through public telephone booth was beyond the defendant's personal expectations of privacy which may be justified by upholding societal standards. The Fourth Amendment's expectation of privacy test and the reasonableness requirement are both invoked in response to a privacy claim. As a result, privacy issues in the US are evaluated according to the norms of a neutral third party with acceptable sensibility.

The US Supreme Court has also validated individual's privacy rights with regard to issues like birth control[97], same-sex relationship[98] and abortion[99] as a penumbra of rights derived from or implied by the constitution. These validated privacy rights are also known as "unenumerated" rights.[100]

4.2.2 TORTS INVOLVING PRIVACY

The majority of states have enacted privacy torts which provide fundamental privacy rights in the US by common law, statute or state constitutional interpretation.[101] The following are examples of privacy torts: invasion of privacy, public revelation of personal information, appropriation and false light. The aforementioned torts protect four different rights of persons, each of which centre around "the right to be left alone" as Samuel Warren and Louis Brandeis distinctly stated in an 1890 law review paper.[102] The scope of privacy torts has been restricted by the First Amendment as well as the reasonableness standard established by US common law.[103]

[97] Griswold v Connecticut, 381 U.S. 479 (1965)
[98] Lawrence v Texas, 539 U.S. 558 (2003)
[99] Roe v Wade, 410 U.S. 113 (1973)
[100] Helscher D, Griswold v. Connecticut and the unenumerated right of privacy, 15 N Ill U L Rev 33–61 (1994)
[101] Elif Kiesow Cortez, Data Protection Around The World-Privacy Laws In Action, 232
[102] Warren and Brandeis, The Right to Privacy, 5 Harvard Law Review, 193 (1890)
[103] Elif Kiesow Cortez, Data Protection Around The World-Privacy Laws In Action, 232

4.2.3 SECTOR SPECIFIC LEGISLATION

The scope or area of control is the foremost distinctive characteristics of US privacy and data security laws. The majority of US privacy laws and regulations have a sectoral focus. For instance, different rules are used for the data processing activities of public and private organisations. [104] Furthermore, different laws apply to firms that operate in various economic sectors or that handle distinct kinds of data. [105] Therefore, sectoral laws defines the proper level of protection for various processing of data activities such as storing medical information, [106] conducting customers transaction and law enforcement. In summary, sectoral regulations threatens to data security and privacy as exclusive to particular categories of information processing businesses or technology. [107]

The following discussion covers the various sectoral data protection laws.

- **"Health Insurance Portability and Accountability Act"**

The HIPAA rules apply to all covered entities that acquire, store, utilise or expose personal health data. Any health data, clearinghouse or healthcare is defined as a covered entity that transmits any health information electronically in connection with a statutory transaction. The Privacy and Security Rules must be followed by Covered Entities in accordance with HIPAA. In accordance with the Rules of Privacy, unless there are certain exceptions or if the patient has not given one's own consent, covered entities are not allowed to disclose protected health data. By imposing sensible and suitable administrative, physical and technical protections, Covered Entities are required to ensure the security, privacy and avaibility of electronic protected health information that they keep or transfer under the security rule.

Both "electronic Protected Health Information" (e-PHI) and "protected health information" (PHI) are recognised under the Act. PHI is protected by HIPPA, however e-PHI is subject to extra rules.

[104] Schwartz P, The EU-US privacy collision: A turn to institutions and procedures, 126 Harv L Rev 1966–2009(2013)
[105] Ibid
[106] Swire P And Ahmad K, Foundations Of Information Privacy And Data Protection: A Survey Of Global Concepts, Laws And Practices. (International Association Of Privacy Professionals, Portsmouth, 2012)
[107] Reidenberg J, Resolving conflicting international data privacy rules in cyberspace, 52 Stan L Rev 1315–1371 (2000)

Information on a person's health that may be identified specifically is protected health information.

(1) Beside what is stated in paragraph.

(2) of the following forms described mainly[108] (i) sent by digital media; (ii) preserved by electronic media; (iii) any other form or content, whether transmitted or stored.

The Security Rule establishes the minimum necessities for all health care groups to: (i) adapt administrative, physical and technical safeguards to maintain the confidentiality, honor and availability of the information; and (ii) disclose security events. [109]

- **"Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003"**

This statute governs the gathering and use of email addresses. It includes all commercial communications as defined by the law which are those that are sent via email and their basic goal is to encourage the use of a commercial good or service, particularly emails that link to content on commercial websites. Commercial emails must include non-deceptive source and topic information, opt-out provisions, the source address and other data that distinctly and prominently recognizes them as solicitations. Under the Act, there are legal repercussions for those who compile email addresses or generate them using a dictionary attack.[110] The CAN-SPAM Act mandates that no organisation, not even 501(c)(3) organisations should send emails with subject lines or messages that are substantially incorrect, false or deceptive.[111] As a result, an email must make it obvious if it is an advertising or an information. The email must distinctly state that the recipient can choose not to receive emails from the sender in the future and it must also contain a way for them to opt out such as a return email address.[112] Emails must

[108] "(2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer."

[109] Eisenhauer MP (2007) Managing your data processors: legal requirements and practical solutions. BNAI's World Data Protection Report. https://www.privacystudio.com/Links%20posted%20to%20web/BNAI%20%20Managing%20Data%20Processo rs%20Aug%2007.pdf

[110] CAN-SPAM Act: A Compliance Guide for Business", Federal Trade Commission. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guidebusiness visited on 15/06/2023

[111] Ibid

[112] Ibid

consist the sender's actual postal address. Lastly, the senders must comply with receivers requests to stop receiving emails from them.[113]

- **"The Fair Credit Reporting Act"[114]**

Consumer reporting agencies, individuals that utilise reports on consumers (say lenders) and organisations that provide information about consumers (a credit card company) are all covered. Any information provided by a CRA on a consumer's reliability, credit record, credit capacity, character, and overall reputation is referred to as a consumer report and is used to determine the consumer's eligibility for loan or policy.[115] To ensure that the material is accurate, a CRA must adopt reasonable processes. A CRA must quickly update any data that is unreliable, incomplete or unable to be confirmed.

- **"Electronic Communications Privacy Act, 1986"**

It restricts the use of recordings on other people's communications without a court's permission or the consent of the party being monitored. It also restricts the use of and disclosure of any data obtained by unauthorised digital monitoring or surveillance.[116]

- **"Computer Fraud and Abuse Act, 1986"**

It aims to deter and penalise hacking related actions which are defined under the Act as unauthorised access to computers that are under protection.[117] The Act also prohibits people or organisations from extending the range of their authorised access.[118] Computers utilised by financial organisations, the US government and anyone involved in or impacting international trade or communication are all protected computers.[119] According to the Act, damage refers to any harm to the accessibility or authenticity of data, a programme, a system or information.[120]

[113] Ibid
[114] 15 U.S.C. §1681
[115] 15 U.S.C. § 1681(d)(1)
[116] Doyle C (2012) Privacy: an overview of the Electronic Communications Privacy Act. Congressional Research Service, p i. https://www.hsdl.org/?view&did¼725508 accessed on 15/06/23
[117] 18 U.S.C. § 1030.
[118] 18 U.S.C. § 1030(e)(6).
[119] 18 U.S.C. § 1030(e)(2).
[120] 18 U.S.C. §1030(a)(5).

- **"Family Education Rights and Privacy Act, 1974"**

All educational organisations and institutions including non-profits that get the necessary funds from the U.S. Department of Education are subject to the Family Educational Rights and Privacy Act[121] (FERPA) which safeguards the information contained in student's school records. According to this legislation, "educational records" are records, data, papers, and other materials that are kept by an educational agency or institution or by a person working on its behalf which include details that is pertinent to a student. Any organisation or institution, whether either private or public, that receives funding through a relevant government programme is referred to as an educational agency or institution.

According to FERPA, every institution that accepts government funding for education is required to give parents of a student and if a student is above 18, the student themselves, the opportunity to see and examine the student's academic records. Every educational organisation or institute is required to set up the relevant processes for approving such requests within a fair amount of time, however in no case more than 45 days after the request is submitted. Furthermore, FERPA requires an educational organisation or authority obtain authorization in writing from a parent, guardian or eligible student prior to disclosing academic records or personally identifiable details included therein to any person, authority or organisation aside from a list of people who are expressly prohibited from receiving such information and associated state officials or agencies.

- **"Children's Online Privacy Protection Act, 1998"[122]**

The COPAA was created to protect children below the age of thirteen if they engage in online platforms by regulating how websites collect, use and publish private data concerning them. In accordance with COPPA, a website host is required to notify the parent regarding its collection of data practises and obtain permission before gathering any information from children. COPPA is applicable with regard to websites intended for children and sites intended for audiences that if its administrator has actual information that the website gathers children's private data.

[121] 20 USC § 1232g
[122] 15 U.S.C. §§ 6501

- **"Gramm-Leach- Bliley Act, 1999"**

According to the GLBA, financial institutions have to maintain the private information of their consumers and safeguard the privacy and security of their non-public personal data. Financial institutions have the right to disclose personal data to other businesses if doing so is required to provide the requested financial services. To credit reporting or financial regulatory agencies, information might be disclosed.

4.2.4 "The Federal Trade Commission"

In order to protect American consumer's privacy, the FTC supervises the handling of personal information in the country.[123] The Federal Trade Commission Act's Section 5 principally allows it to accomplish this since it grants it the power to maintain independent monitoring of and take enforcement action against unfair and misleading business practises.[124] The FTC currently controls the administration of privacy regulations and has the authority to impose orders and monetary penalties against companies that violate customers right to privacy.[125] While the FTC has been praised for changing the behaviours of large firms, it has also come under criticism for its inaction in response to activities that have drawn harsh criticism and compromised privacy such as Facebook online tracking practises.[126] For federal privacy legislation including GLBA, FCRA, and COPPA, the FTC is the main enforcement body. By issuing consent decrees as part of agreements with businesses accused of breaking privacy regulations, it has become more proactive in recent years in defending consumer privacy.

In addition to these federal laws, there are several state statutes. The California Consumer Privacy Act (CCPA) is the one that is most important among them.

"California Consumer Privacy Act"[127]

The implementation of California's CCPA, a comprehensive privacy rule that detractors had quoted as California's GDPR, it has been the most significant latest privacy development in

[123] Hoofnagle C, Federal Trade Commission Privacy Law And Policy, (Cambridge University Press, New York , 2016)
[124] 15 U.S.C § 45.
[125] Solove D, HartzogW, The FTC and the new common law of privacy, 114 Colum L Rev 583–676 (2014)
[126] Elif Kiesow Cortez, Data Protection Around The World-Privacy Laws In Action, 232
[127] The California Consumer Privacy Act (CCPA), A.B. 375, 2017 General Assembly, Reg., Session, (Cal.2018)

United States so far. The CCPA is having a great influence and businesses across the US and the rest of the countries are assessing what it means for them in light of California's size and the importance of Silicon Valley being there.[128]

The most comprehensive privacy or data protection regulation in the nation was instantly established upon the CCPA's implementation on January 1, 2020. For profit companies that conduct trade in California and fall into one of three size groups are subject to the CCPA's regulations if they gather or control how private data is dealt with. Businesses that collect personal information from residents of California are subject to strict rules regarding disclosure on their privacy policies. It mandates that companies provide Californians the right to view and erase their private data as well as the option to stop the data from being disclosed to unknown parties. It prohibits businesses from disseminating personal information about minors without receiving their explicit authorization. The CCPA establishes a personal right of action for specific breaches of data brought on by the failure of an organisation to adhere to and uphold adequate security standards and procedures. The California Attorney General is empowered to impose statutory fines of up to $7,500 per violation in order to implement the CCPA's provisions.

4.3 DATA PROTECTION IN UK

Before 2016, the Data Protection Act of 1998[129] (DPA 1998) served as the principal data protection law in the UK. The DPA 1998 was passed for the enactment of the 1995 EU Data Protection Directive (DPD) into UK domestic legislation.[130] The DPD was replaced in 2016 by the EU's General Data Protection Regulation (GDPR).[131] After the UK left the European Union, the UK government incorporated the General Data Protection Regulation (Regulation (EU) 2016/679) into UK national law (creating the "UK GDPR"). The GDPR has gone under

[128] Alen Charles Raul, The Privacy, Data Protection And Cyber Security Law Review, 416 (The Law Reviews, 2019)
[129] Data Protection Act, 1998
[130] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
[131] 2Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1. After the transition period of the UK's withdrawal from the EU, the 'UK GDPR' will replace the GDPR in the UK – the UK GDPR is essentially the GDPR converted into domestic legislation: see The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, sch 1.

numerous technical improvements in the UK to reflect its position as a national legislation of the country (such as replacing references to "Member State" with "the United Kingdom"). These amendments were carried out in accordance with the Data Protection, Privacy, and Electronic Communications (Amendments and Other Provisions) (EU Exit) Regulations 2019. For the time being, all significant responsibilities placed on controllers and processors under the EU and UK GDPR are substantially the same.[132] In the United Kingdom, the Data Protection Act of 2018 (commonly known as the "DPA") is still in force as a supplementary national data protection legislation. It conveys issues that were addressed before by exclusions and derogations from the EU GDPR (such as compelling people's interest justifications for the processing if particular category data and circumstance specific exemptions from GDPR requirements like data subject rights).[133] Despite a few changes, the new data protection framework established by the GDPR and DPA 2018 is generally comparable to the one it replaced.[134] The DPA 2018 can be divided into six key sections: general processing, law enforcement processing, intelligence service processing, UK data supervisory authority, Information Commissioner's Office (ICO), enforcement, supplemental and final provisions and the UK data supervisory authority. The Privacy and Electronic Communications (EC Directive) (Amendments) (Regulations) (Regulations) (PECR), which was updated by the Privacy and Electronic Communications (EC Directive) (Amendments) (Regulations) (Regulations) 2011 (PECR), regulates not only the use of cookies as well as other comparable technological devices but also the processing of location and traffic-related information. The European Commission published a draught of the proposed Regulation on Privacy and Electronic Communications (ePrivacy Regulation) to replace the current ePrivacy Directive. The UK's compliance with the eRegulation in the post-Brexit situation is uncertain because it has not yet taken effect.

The main changes made by the proposed ePrivacy Regulation will be:

a) Increasing challenges in getting authorization for cookies.
b) to make website browsers responsible for seeking authorization for the usage of cookies.

[132] Data Protection Laws of the World, DLA Piper, 883
[133] Ibid
[134] Benjamin Wong, The journalism exception in UK data protection law, 12:2, Journal of Media Law, 216-236, (2020)

c) Increase the difficulty of obtaining consent for direct marketing and mandate that it follow to GDPR standards; however, it's probable that current exclusions will be kept.

The Data Protection Act, 2018 control how organisations, the government and companies use private data. Four separate "data protection regimes" are established in the UK by the four parts of the Data Protection Act 2018:

1. The first section is organised around the European GDPR and supplements and adapts it to UK domestic legislation.
2. The EU GDPR is expanded upon in Part 2 and modified in some circumstances so that it can be applied to UK law in a different way.
3. For law enforcement agencies, part three establishes a new and distinct framework.
4. A new and distinct framework is established in Part 4 for the UK's intelligence services.

The Data Protection Act of 2018 also incorporates key terms from the EU GDPR[135] including:

- Data that may be used to locate or reach a live individual is considered personal data[136].
- Processing[137] is defined as any action taken in relation to information, including gathering, recording, storing, disclosing, combining, etc.
- The term data subject[138] refers to a live person to whom private information pertains.
- A controller or processor[139] is any natural or juridical person, governmental body, authority or other legal entity that decides either independently or together with others, its purposes and techniques of collecting personal information.

4.3.1 PRINCIPLES OF DATA PROTECTION

The Data Protection Principles are a set of guidelines established by the DPA. Thesse are as follows:

1. The fundamental data protection principle is that any use of private information for law enforcement purposes must be legitimate and fair.[140]

[135] Sec 5 of the DPA, 2018
[136] Sec 3(2) of the DPA, 2018
[137] Sec 3(4) of the DPA, 2018
[138] Sec 3(5) of the DPA, 2018
[139] Sec 3(6) of the DPA, 2018
[140] S. 35 of the DPA, 2018

2. According to the second criteria, the reason for collecting data must be distinct, lawful, and explicit.[141]
3. The third data protection rule states that private information collected for any of the law enforcement objectives must be appropriate, pertinent and not excessive in connection to the reason for which it is collected.[142]
4. The deletion or correction of erroneous personal data is covered under the fourth principle.[143]
5. The retention of personal information for any law enforcement purpose shall not exceed the time required by that purpose according to the fifth data protection principle.[144]
6. The sixth data protection rule states that any law enforcement-related processing of private information must be done in a way that protects the safety of the data, using the proper organisational or technological safeguards.[145]

4.3.2 INFORMATION COMMISSIONER'S OFFICE

The Data Protection Act recognises the Information Commissioner's Office (ICO)[146] as the primary data protection body in the United Kingdom. The ICO's role, authority, function and powers are defined in the Act.[147] The DPA 2018 is enforced by the ICO which also has the authority to impose over businesses that adhere to the GDPR'S data security needs.

The ICO is autonomous and accountable for:

a) keeping a record of controllers in the public.
b) promoting best practises by giving safeguarding guidance and support as well as collaborating with enterprises to improve their data handling practises by inspections, consulting visits and information security workshops.
c) deciding on complaints.
d) taking disciplinary action.

[141] S. 36-The second data protection principle
[142] S. 37 of the DPA, 2018
[143] 7 S. 38- The fourth data protection principle
[144] S. 39 of the DPA, 2018

[145] S. 40 of the DPA, 2018

[146] S. 114 of the DPA, 2018
[147] S.115 and 116 of the DPA, 2018

4.3.3 PRIVACY AND DATA RIGHTS SUBJECT

Similar to those in the EU GDPR, data subjects have a list of rights that they may use to control how their private information is collected. Controllers are given a period of one month to report or submit information on actions done in response to request. If the request is particularly onerous, however, the controller may be able to extend this deadline by a further two months.

- Right of access[148]

  An individual has the right to request access to as well as a copy of his or her private information as well as the necessary details regarding how the controller has utilised the information.

- Right to rectify[149]

  The right of data subjects to have incomplete or incorrect personal information to be corrected as quickly as feasible.

- Right to erasure (right to be forgotten)[150]

  Individuals with personal data have a right to have it erased. The right is conditional and only applies in certain situations, for instance if the controller no more necessitate the information for the reasons for which that they were obtained or otherwise legally examined or as a result of the controller successfully exercising their right to object or withdraw their consent.

- Right to restriction of processing[151]

  The right to regulate how their personal data is processed exists in some circumstances. These include circumstances in which the data's correctness is disputed, the processing is

[148] Article 15 of EU GDPR and Art 45 of DPA, 2018
[149] Article 16 of EU GDPR and Art 46 of DPA, 2018
[150] Article 17 of EU GDPR and Art 47 of DPA, 2018
[151] Article 18 of EU GDPR and Art 47 of DPA, 2018

unlawful, the data are no longer required save for the purposes of the data subject's legal rights, or the controller's legal justifications for processing the data are in doubt.

- Right to data portability[152]

The subject has the right to obtain all of one's own private information from the controller or to appeal that it be transmitted to another controller in an arrangement, generally acknowledged and machine readable format in cases where the processing of private information is justified by the subject's consent to the processing or by the requirements of the processing for the fulfillment of a contract.

- Right to object[153]

Data subjects have full-fledged rights to object to the processing of their data when it serves the people's interest or based on legitimate interests of the data controller. Controllers must stop collecting information until they can prove they have compelling, valid reasons to do so that outweigh the rights of the data subject. Therefore, individuals have the unrestricted right to object to have their private data used for direct marketing.

- The freedom from being subjected to profiling and other automated decision making[154]

Only when it is necessary for entering into or closing a contract, authorised by UK law or the data subject has provided express (i.e. opt-in) authorization is automated decision-making including profiling, that materially affects the data subject allowed.

4.3.4 ENFORCEMENT AGENCIES

In accordance with the DPA 2018, the ICO is given a number of enforcement capabilities including the ability to monitor and enforce both the GDPR and the DPA 2018 in the UK. Among these surveillance and regulation authorities has the power to:

[152] Article 20
[153] Article 21
[154] Article 22 of EU GDPR and Art 49 of DPA, 2018

a) information notices[155]: obtaining information from controllers that the commissioner technically needs in order to assess compliance with the GDPR or the DPA 2018 and requiring controllers and processors to give the ICO with such data.
b) assessment notice[156]: necessitates the controller to provide the ICO the authorization to conduct an examination of their compliance with the GDPR or DPA 2018.
c) notice of intent[157]: if the ICO notifies the controller or processor of its intention to penalize them for violating the DPA 2018 or GDPR after conducting an investigation. This sort of notice provides the controller the opportunity to make representations and outlines the ICO's points of concern regarding suspected GDPR or DPA 2018 violations. After carefully evaluating these statements, the ICO releases an enforcement notice as its end decision on any impose of action.
d) enforcement notices[158]: These notices are sent out when the ICO determines a controller or processor has violated the DPA 2018 or the GDPR, laying out the consequences of non-compliance which may involve a possible prohibition on processing any sort of particular categories of personal data.
e) penalty notices[159]: If the ICO discovers that a controller or processor has breach the GDPR or the DPA 2018 or has ignored an information notice, assessment notice or enforcement notice, the ICO may, by notice, seek the payment of a fee for the breach of the GDPR or the DPA, 2018. The GDPR permits fine up to €20 million or 4% of yearly global revenue.

Although it is still unclear how data protection laws will be governed in the UK after Post-Brexit, it is anticipated that the EU GDPR will continue to have legal ramifications there until the UK government passes legislation repealing its provisions and negating its legal significance in UK law, as well as amending the DPA 2018's provisions. This is because the GDPR took effect before the UK was supposed to leave the EU.

[155] Sec 142-145 of DPA, 2018
[156] Sec 146 and 147 of DPA, 2018
[157] Schedule 16 of DPA, 2018
[158] Sec 149-153 of DPA, 2018
[159] Sec 155-157 of DPA, 2018

4.4 DATA PROTECTION IN INDIA

In India, there is no explicit regulation that governs data privacy at present. The Information Technology Act of 2000 is the only law that addresses cybercrimes and offers sanctions for breaking the law. Despite the fact that the legislation only has a few privacy related clauses, they are not all inclusive.

Under section 43A[160], if a body corporate negligently fails to implement and maintain reasonable security practices to protect sensitive private information or data of an individual and causes improper harm or unlawful benefit to any person, then that body corporate may be required to compensate to that individual. It is important to note that the act does not specify a maximum limit for the amount of compensation that can be sought by the aggrieved party in such situations.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, govern the security of a person's private information or sensitive personal data, which includes personal data pertaining to:

- Passwords
- Details on financial accounts, credit card, debit card, and other payment methods details
- Sexual orientation
- History of medical records
- Biometric information

Section 72 of the act[161] states that anybody who attains access to any electronic record, book, register, correspondence, information, document or other material without the will of the individual's concerned and discloses that information without the individual's knowledge or will while acting under the authority granted by the IT Rules or Regulations made thereunder is subject to imprisonment for a term of up to two years and a fine up to Rs. 1,00,000/- or both.

Under section 72A[162], disclosure of information without the subject's consent and in breach of a valid contract makes it illegally and doing so is punishable by up to three years in imprisonment and a fine of Rs. 5,00,000/-.

[160] Section 43A of the Information Technology Act, 2000
[161] Section 72 of the Information Technology Act of 2000
[162] Section 72A of the Information Technology Act, 2000

4.4.1 DIGITAL PERSONAL DATA PROTECTION BILL 2022

Ministry of Electronics and Information Technology (MEITY) issued a draft of an amended legislation called the "Digital Personal Data Protection bill, 2022" which had six chapters and thirty parts. The Bill has not yet been submitted to the parliament and is still only a draft.

4.4.2 CHARACTERISTICS OF THE BILL

1. **TERRITORIAL APPLICABILITY:** The Bill governs the processing of digital personal data inside India's borders, including data gathered online. It expands its scope to the processing of private information beyond India provided that such processing is done for the purpose of selling goods or services or profiling persons inside India. Any information that may be used to identify a specific person is considered personal data and processing is any automated procedure or set of computerised processes that are carried out on digital personal data which includes but is not limited to gathering, storage, use and distribution.

2. **CONSENT:** The legislation stipulates that a person must give authorization in order for their personal information to be used for a legitimate purpose. A written notice that provides specifics about the personal data that will be gathered and its intended uses must be provided prior to requesting consent. It's crucial to keep in mind that authorization may be revoked at any time. But permission is not always required. For example, processing may be required in order to fulfil a legal obligation, deliver a government service or benefit, deal with a medical emergency, obtain a job or carry out other activities that serve the public interest, such as preserving information security or preventing fraud. A person's legal guardian must provide authorization if they are below 18 years

3. **Rights and Duties of Data Principal:** The data principal or that individual whose information is being dealt with, has specific rights with regard to data processing. These rights encompass the entitlement of individuals to be informed about the utilization of

their data, the ability to request amendments or removal of their personal information, the option to designate a representative to exercise their rights in case of incapacity or demise, and the right to seek remedies for any grievances. Conversely, data leaders bear certain obligations that they must fulfil. These obligations entail refraining from lodging fraudulent or frivolous complaints, providing false data, concealing information, or assuming false identities in specific circumstances. Failure to adhere to these responsibilities could result in fines of up to Rs. 10,000/-.

4. **Obligation of Data Fiduciaries:** In compliance with data protection regulations, the entity responsible for determining how data is processed, known as the data fiduciary, has certain obligations to fulfill. These obligations include taking reasonable measures to ensure the accuracy and completeness of data, implementing appropriate security measures to prevent data breaches and informing the Data Protection Board of India and affected individuals if a breach occurs. Furthermore, the data fiduciary must stop retaining personal data once its purpose has been fulfilled and there is no longer a legal or business need for it, as specified by the storage limitation requirement. It is important to mention that government entities involved in data processing are exempt from this requirement.

5. **TRANSFER OF PERSONAL DATA OUTSIDE INDIA:** The Indian government intends to inform countries when a data fiduciary transfers personal data to them. These transfers will be subject to specified terms and conditions set by the government.

6. **EXEMPTIONS:** The proposed legislation includes specific situations where the rights of individuals and the responsibilities of organizations handling data will not apply, except for data security. These exceptions are relevant when preventing and investigating crimes or when enforcing legal rights or claims. Furthermore, the government has the power to exempt certain activities from the provisions of the legislation by issuing official notifications. These activities could involve data processing by government entities for the purpose of state security and public order, as well as research, archiving, or statistical purposes.

7. **DATA PROTECTION BOARD OF INDIA:** The Indian government plans to create the Data Protection Board of India, tasked with ensuring adherence to data protection laws and imposing penalties for violations. The Board will also possess the authority to issue instructions to data stewards regarding data breaches and address grievances from affected individuals. The government will determine the composition of the Board, the selection process for its members, their tenure and terms of service, as well as the procedure for their removal.

8. **PENALTIES:** The timetable of the Bill specifies the repercussions for various infractions, which include a highest possible fine of Rs 150 crore for disregarding responsibilities related to children, and a maximum fine of Rs 250 crore for not implementing measures to safeguard against data breaches, with the potential to exceed up to 500 crores. Prior to imposing penalties, an investigation will be carried out by the Board.

4.5 CONCLUSION

Although experts may regard America's privacy protection framework to be weaker than the European approach, in certain ways, the American system provides more safeguards than the European counterpart.[163] Swire and Kennedy-Mayo contend that

In various ways, American safeguards are more stringent:

1. Supervision of searches by judicial officials.
2. For both physical and digital searches, the probable cause of a crime is a reasonably stringent criteria.
3. Significantly more stringent guidelines on the use of real-time intercepts by the government such as telephone wiretaps.
4. Civil cases reinforce the exclusionary rule which prevents prosecutors from using improperly obtained evidence.

[163] Dario Maura Vincete & Sofia De Vasconsels, Data Protection In The Internet, (Global Studies In Comparative Law, Springer 2020)

5. Other legislative requirements that are quite rigorous for government access in various non-search circumstances such as the judge-supervised reasonable and articulable suspicion level under the ECPA.
6. Transparency standards, such as informing the service provider of the request's legal justification.
7. Absence of data preservation regulations for communication via the internet.
8. Absence of restrictions on the usage of secure encryption.

The predominant strategy in the United States is based on consumer protection laws, as compared to the European Union's data protection strategy which in many respects serves as the gold standard of privacy safeguards. The UK legislation's Privacy Principles and Data Protection Principles can be viewed as a strong way of protecting private information. Despite being complicated and expensive, the sectoral law in the US has the benefit that practically everything is covered more effectively.

CHAPTER-5

CONCLUSION AND SUGGESTIONS

5.1 FINDINGS

Economic advancement demands innovation based on data. We can easily be persuaded as a society to give away our personal data so as to take advantage of applications that track every step we take. It is almost difficult to refuse to be part of it. In today's world, privacy laws would completely protect consumers, giving them little negotiating power but simultaneously promoting economic progress. There is a greater chance of privacy invasion no matter how digitalized our daily activities have become or sometimes without being aware of it. The entire world is presently experiencing a number of challenges as an outcome of the development of various social networking projects and artificial intelligence-controlled technological advances. These challenges are going to grow as technologies evolves and innovative apps become available more frequently in the decades to come.

Following are the key challenges that the data protection strategy has to overcome:

1. **DATA PROVIDED VOLUNTARILY:** The prevalence of provided data, especially due to the emergence of portable gadgets and social media networks is the initial obstacle to protecting one's data privacy today, despite the fact that operators of such gadgets might not think of themselves to be contributing information to others. The emergence of the quantified self or the self-monitoring of biological, ecological, physical or behavioural information using gadgets that track, Internet-of-things devices, social networking data and others could result in information being acquired about users individually as well as about those in their immediate surroundings. Therefore, depending just on authorization to secure one's information is inadequate particularly considering that information collected for a particular reason might be used for other purposes.

2. **PROFILING:** The quantity and kind of information that is obtained about them and also how these details can be used to infer their features utilising technology based on AI tends to be unknown to the data subjects. The fact that consumers have no choice over the way they are categorised or how their connected gadgets will respond to them as a consequence of this kind of profiling which is a serious problem.

3. Research has shown that such information targeted can result in people having too much faith in their own opinions, which may cause violence and divisiveness in society. Research on data privacy and protection should focus on possible solutions to this issue in the future.

4. **CONDITIONING:** A global infrastructure of behavioural change is expected to endanger humanity in the 21st century much like industrial capitalism did in the twentieth when it destroyed the natural world. Tools associated with computer technology have the ability to influence human behaviour and change people into whatever the capitalists desire.

5. **SURVEILLANCE CAPITALISM:** In her book *"The Age of Surveillance Capitalism: The fight for a Human Future at the New Frontier of Power", Soshanna Zuboff* outlines surveillance capitalism, a business paradigm that supports the digital world.[164] It requires an innovative kind of capitalism that continues through providing empowered services to countless people enabling consumers to observe their users conduct in incredible detail often without their express permission. According to Zuboff, surveillance capitalism simply regards the experience of people as a source of unrestricted data on activity. Although a limited amount of this information has been utilised to improve service to customers, the majority is classified to be private behaviours and used in advanced manufacturing processes known as "machine intelligence" for creating goods for prediction that believe what individuals will

[164] Zuboff, Shoshana. The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power (New York: Publicaffairs, 2019)

conduct now and in the years to come. Lastly, such tools for predicting are being sold in behavioural markets for futures, an emerging kind of trade. As an outcome of their transactions, surveillance capitalists are making significant amount of money because of the fact that many companies have agreed to stake their future on their conduct.

5.2 CONSENT BASED APPROACH

The majority of privacy legislation throughout the world are “consent-based.” The GDPR and the recently introduced data protection Bill both have a basis with the “consent model” of safeguarding privacy. The information controller has the right to acquire, manage, and execute the data with the individual’s consent for the stated reason and is not accountable for any consequences that could result from its actions. Therefore, it is the person’s responsibility or duty to be informed of the terms of the data access that an individual is authorized with. As a result, data controllers are favored above data subjects.

Since, the Consent Model was enough or adequate and there weren’t ample grounds to gather data and few uses that could be further created of it in the upcoming period. After the data had been collected and became static, the other parties could rarely get access to the data. As a consequence, it was easy for data subjects to know what information was being collected and how data would be utilised and enabling users to make wise decisions. In this case, the consent model proved appropriate and feasible.

However, things are different now. Our online actions are being watched and with each google search, facebook or instagram click, twitter tweet or purchases made online, our identity is being established and we are constantly being surveillance or trace which we haven't been aware about are to be categorised into classifications. Advanced technologies like smart gadgets with sensor detects and cyber intelligence have surrounded us, monitoring our every movement. Furthermore, there is a remarkable imbalance of power between controllers and the information consumers. As we are required to agree a certain form of "contract" of consent without agreeing to which we cannot able to access the service provided by the data controller. Individuals consent to this information obtained by signing lengthy, complicated, standard agreements that are difficult to comprehend. As a result, a data subject's position is weakened.

5.3 DATA PROTECTION LAW BASED ON THE RIGHTS MODEL

To overcome the drawbacks of the consent based method, the rights based approach offers a strong substitute. The rights model, contrary to the consent model, guarantees the interests of the information's subject, and those who manage the data are now liable for maintaining the secrecy of the information. The concept of privacy emphasises that individuals have a basic right to their confidential data. The concepts of independence, protection and responsibility form the foundation of rights based approaches.

The person who is the controller of the data must be liable for any data in their possession, without regard to whether the information's user has consented. Every one of the data users are entitled to control regarding their data and in cases where they are unable to effectively stop data collection, individuals should be given the choice to limit or restrict how their data is handled. Data must be handled securely at all stages of gathering, the process, usage, and removal.

Following are some consequences of the rights based framework:

- Each individual holds certain inviolable power over their own private information. Data controllers have a duty for protecting these rights. The individual who is in charge of maintaining the data has responsibility for any harm that results from their conduct and owes a responsibility to exercise caution to the information under their management.

- The personal information controller is liable for any damage done to the data user. The rights based model detects possible damages and proposes solutions.

It is not argued that the rights related framework is safe but instead that it is better than the consent based method of safeguarding information.

5.4 NECESSITY OF A GLOBAL DATA PROTECTION STANDARD

That we are currently witnessing a significant generational change in the regard for privacy. This reform has been implemented in order to develop feasible morals for an increasingly digital world. The dynamics of socio technological change and economic globalisation are the reason for such change. It is being pushed by the digitalisation of practically everything in our business and service sector, as well as our social ties, governance, and administration. It is mostly determined by the possibility for shifting decisions made by humans, responsibility,

and disclosure to automated machines. Digitisation knows no geographical limitations. It is insensitive to human limits such as whether we intend information to remain open to everyone, confidential or somewhere in between. It infiltrates our most private interactions, discussions, and areas of interest. The privacy paradox is not that individuals have different reasons to reveal and hide information. The paradox is that the new opportunities and vulnerabilities created by rapid digitization are not yet well understood by us. What does ethics mean? Ethics is the intuitive feeling that all individuals possess, often subconsciously, of what is good and wrong in certain situations. But this type of ethical approval is absent in the modern digital environment.

There is a dire need for international laws regulating safeguarding information norms. It is not easy for companies to maintain compliance with the various data privacy laws in each country. As the territories change, they are compelled to modify their data protection laws and regulations. Two drawbacks are therewith the same. One, there is no consistency in the rights guaranteed in different countries. Furthermore, it would be difficult to write different privacy rules for the same organisation in different nations. With shifting privacy standards, organisations must devote more effort to updating their policies, which, yet again is not possible.

GDPR is now the only legislation that has been broadly enforced. Though, it cannot be seen as a worldwide one. To determine what constitutes good data protection laws, there needs to be a standard for data protection that is applied internationally. To maintain consistent data security over industries and promote powerful unified data security compliance with the legislation a clear, realistic and internationally applicable enough criterion is required.

5.5 INDIA'S DATA PROTECTION LAW

India currently is regulated by the framework of the IT Act and IT Rules that fall lacking in both the current needs and the rapid development of information technology as it lacks adequate laws governing data protection. However, India's first data protection law is the planned Data Protection Bill, 2022. Therefore, it is clear that India lacks a sufficient data protection law. If the present bill is enacted, it will safeguard and facilitate data protection. The Digital Personal Data Protection Bill of 2022 is a bill that will give India authority over personal data. All organisations that manage the personal data of Indian citizens are required under the bill to comply with its obligations. The Act applies to all organizations including the

government, private companies and non-profit organizations that handle personal data. The tendency towards data localization is likely the cause of the absence of data localization regulations in the legislation. The law establishes clear guidelines for data management and imposes severe penalties on companies that fail to adequately secure customer information. The proposed regulation is compatible with international norms for the security and privacy of data such as the General Data Protection Regulation (GDPR) which emphasises the need of obtaining individuals informed approval prior gathering and storing data about them.

The hypothesis of the research "The privacy of people in relation to their personal information in cyberspace is not sufficiently safeguarded under Indian legislation" the hypothesis set has not been proven to be true. Since India has legislation for the protection of data such as the Information Technology Act of 2000 and the newly put forth Digital Personal Data Protection Bill 2022. However, complete privacy protection continues to be inadequate in India and it is clear that India is continually working to pass a data protection law and the regulatory framework.

5.6 SUGGESTIONS

5.6.1 NATIONAL LEVEL

- The right to data privacy should be declared and proclaimed a constitutional right since adopting so would require the government to uphold, protect and sustain the right on behalf of all people including those with disadvantages who might not be able to get safeguard on their own behalf.

- The Data Protection Bill 2022 is needed to be approved in order to guarantee that its laws may be enforced even against the State.

5.6.2 GLOBAL LEVEL

- The right to privacy in information has to be considered as an inherent human right and global organisations must provide principles for safeguarding information which may serve as the basis of various state laws.

- It would be ideal if there were an international law on the principles that underlie the many data protection regulations in place across the world as data transcends national and continental borders.
- Globally, nations could adopt the rights based concept of data protection legislation.

Difficult to implement, the government must make room for a digitalized future because of the advantages it will bring but they should not do so at the expense of peoples fundamental right to privacy.

BIBLIOGRAPHY

ARTICLES

- Adam D. Moore, Toward Informational Privacy Rights, 44 San DIEGO L. REV. 809 (2007)
- B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014)
- Benjamin Wong, The journalism exception in UK data protection law, 12:2, Journal of Media Law, 216-236, (2020)
- Bratman, B. E.: Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy,69 Tennessee Law Review 344 (2002)
- Charles Fried, Privacy, 77 Yale L. J., Vol.77, 475 (1968)
- Christina P. Moniodis, Moving from Nixon to NASA: Privacy's Second Strand- A Right to Informational Privacy, 15:1Yale Journal of Law and Technology 154, (2012)
- DeVries W, Protecting privacy in the digital age, 18 Berkeley Tech LJ 283–311(2003)
- Diane P. Michelfelder, The moral value of informational privacy in cyberspace, 3 Ethics and Information Technology 129–135, (2001)
- Edward Lee, "The Right to be Forgotten v. Free Speech" Journal of Law and Policy for the Information Society, 103 (2015)
- Felicia Lamport, "DEPRIVACY", Look Magazine, 1970.
- George B. Trubow, Protecting Informational Privacy in the Information Society, 10 N. ILL. U. L. REV. 521 (1990).
- Helscher D, Griswold v. Connecticut and the unenumerated right of privacy, 15 N Ill U L Rev 33–61 (1994)
- James Madison, Essay on Property, in Gaillard Hunt ed., 6 The Writings of James Madison 101-103, (1906).
- Laura Bradford, Mateo Aboy, Kathleen Liddell, A Stress Test for Privacy, the GDPR and Data Protection Regimes, Journal of Law and Biosciences, 25 (2020)
- McGeveran W, Friending the privacy regulators. 58 Arizona Law Review. 959-961, (2016)

- Michael C. James, A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe, 29:2, Connecticut Journal of International Law, *261* (Spring 2014)

- Mike Wagner & Yun Li-Reilly, The Right to be Forgotten, 72:6 The Advocate, Nov. 2014
- Moira Paterson & Maeve McDonagh, Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data, 44 Monash University Law Review 1 (2018).
- Nishant Shah, Identity and Identification: The Individual in the Time of Networked Governance, 11 Socio-LEGAL REV. 22 (2015).
- Nuala O'Connor, Alethea Lange and Ali Lange, *Privacy in the Digital Age,* Great Decisions, 19, 17-28(2015),
- Padmini Ray Murray & Paul Anthony, Designing for Democracy: Does the Personal Data Protection Bill 2019 Champion Citizen Rights? Vol. 55:21 Economic and Political Weekly, (2020)
- Prosser, W.: *Privacy, 48:3* California Law Review, 384 (1960)
- Reidenberg J, Resolving conflicting international data privacy rules in cyberspace, 52Stan L Rev 1315–1371 (2000)
- Richard A. Posner, Privacy, Surveillance, and Law, *75* University of Chicago LawReview 245 (2008)
- Schwartz P, Solove D, Reconciling personal information in the United States andEuropean Union, 102 Calif L Rev 877–916 (2014)
- Solove D, Hartzog W, The FTC and the new common law of privacy, 114 Colum L Rev583–676 (2014)
- Terry N, Existential challenges for health care data protection in the United States, 3Ethics Med Public Health 19 (2017)
- Warren and Brandeis, The Right to Privacy, 5 Harvard Law Review, 193 (1890),
- Weber, Rolf H. The right to be forgotten." More than a Pandora's Box, 2 Journal ofIntellectual Property, Information Technology and E-commerce,120-130 (2011)
- Yvonne McDermott, Conceptualizing the right to data protection in an era of Big Data,Big Data and Society 1, (2017)

BOOKS

- Alen Charles Raul, The Privacy, Data Protection And Cyber Security Law Review, 374 (The Law Reviews, 2019)
- Arthur R. Miller, The Assault On Privacy, 39 (Ann Arbour, Michigan University Press, 1971)
- Daniel J Solove, The Digital Person, 26 (New York University Press, 2004).
- Dario Maura Vincete & Sofia De Vasconsels, Data Protection In The Internet, 412 (Springer 2020)
- Elif Kiesow Cortez, Data Protection Around The World-Privacy Laws In Action, 232 Dario Maura Vincete & Sofia De Vasconsels, Data Protection In The Internet, 412 (Springer 2020)
- Hannah Yeefen Lim, Data Protection In The Practical Context, 12 (Academy Publishing, 2017)
- Hoofnagle C, Federal Trade Commission Privacy Law And Policy, (Cambridge University Press, New York , 2016)
- James Waldo, Herbert S. Lin, Lynette I. Millett, Engaging Privacy And Information In A Digital Age 48 (The Academies Press, 2007)
- John Stuart Mill, On Liberty, 13, (Batoche Books 1859)
- Mark Burdon, Digital Data Collection And Information Privacy Law 2 (Cambridge University Press, 2020)
- Neil Richards, Intellectual Privacy-Rethinking Civil LibertiesIn The Digital Age, 104 (Oxford University Press, 2015)
- Swire P And Ahmad K, Foundations Of Information Privacy AndData Protection: A Survey Of Global Concepts, Laws And Practices. (International Association Of Privacy Professionals, Portsmouth, 2012)
- Viktor Mayer Schonberger, Delete: The Virtue Of Forgetting In The Digital Age, (Princeton University Press, 2009)
- William W. Lowrance, Privacy, Confidentiality And Health Research 7 (Cambridge University Press, 2012)
- Zuboff, Shoshana. The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power (New York: Publicaffairs, 2019)

CONVENTIONS

- African Charter of Human and People's Rights, 1981
- African Charter on the Rights and Welfare of the Child, 1990
- American Convention on Human Rights ,1967
- American Convention on Human Rights, 1969
- Convention on the Rights of Child, 1989
- Convention on the Rights of Persons with Disabilities, 2007
- European Convention on Human Rights (ECHR), 1950
- International Convention on the Protection of the Rights of All Migrant Workers andMembers of Their Families, 1990
- International Covenant on Civil and Political Rights (ICCPR), 1966

ONLINE SOURCES

- CAN-SPAM Act: A Compliance Guide for Business, Federal Trade Commission. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam act-compliance-uidebusiness
- A free and fair digital economy, protecting privacy, empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Pg-114, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- African Charter on the Rights and Welfare of the Child, https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf
- Alessandro Acquisti, The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, in Joint WPISP-WPIE Roundtable (OECD, 2010), https://www.oecd.org/sti/ieconomy/46968784.pdf
- Allens, In a nutshell: data protection, privacy and cybersecurity in Australia, Lexology, (October 2020) https://www.lexology.com/library/detail.aspx?g=2027ba56-6178-4e7f-9273-9aa9bb2f5066

- Amber Sinha, *Right to be Forgotten – A Tale of two Judgments*, Centre for Internet Society, https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-judgments
- Anirudh Burman, Will India's Data Protection Law Protect Privacy and Promote Growth? https://carnegieendowment.org/files/Burman_Data_Privacy.pdf