UiO : Faculty of Law
University of Oslo

Data privacy in the largest democracy. Is it a paradox?

Data privacy regime in India. Analysis and comparison of the Data Privacy Regime in India and The European Union's GDPR.

Candidate number: 7005

Submission deadline: 15th August 2022

Number of words: 17050

Contents

List of Abbreviations

GDPR	General Data Protection Regulation
EU	European Union
PDPB	Personal Data Protection Bill
EDPB	European Data Protection Board
ICCPR	International Convention on Civil and Political Rights
UDHR	Universal Declaration of Human Rights
ECHR	European court of Human Rights
ICESCR	International Convention on Economic, Social and Cultural Rights
SCC	Supreme Court Cases
OECD	The organization for economic corporation and development

Acknowledgement

My master thesis journey has been long and almost like a roller coaster ride. It was possible because of the support of my family, friends, and colleagues at work. At the very top of my prodigious list is Dr Cholarajan M., my thesis supervisor, who has been an excellent guide throughout this thesis and provided me with advice and profound ideas. A special thanks to Apar Gupta, a privacy activist who took time from his busy schedule to be interviewed. I humbly thank him for sharing his vast erudition on the topic that is so relevant to modern India. Nonetheless, I am incredibly happy that I had the support and love of my family *(who travelled to Norway to be with me).* This thesis is the result of many months and weeks spent on research and drafting, internships, a full-time job, and the struggles of being a foreigner. In the end, I would like to thank myself for not giving up and pushing myself very hard. It has truly been an honor and pleasure.

INTRODUCTION

Problem statement

'Data' and data privacy is the reason why one should care about the data protection and surveillance laws in their country as well as other countries. As technology advances and becomes more integrated into daily tasks, data has become borderless and easily accessible. Therefore, leading to new challenges in terms of data protection.[1] It was never before that data protection, national security and information privacy have been more important to ensure the fundamental rights of citizens[2]. A considerable amount of shift toward data privacy was also witnessed during the global COVID-19 pandemic. A time that requires the governments to open dialogue about contract tracing and collection of data for protecting public health during a time when the globe was under a health crisis.[3] The nature of data being 'international' led to many problems, for example, covid tracing apps that transferred data from one country to another to store it in the cloud.[4] This further complicated the issue of data privacy because there is no global standard that regulates data transfers. Along with this and many other reasons that we will discuss in the thesis, it has become a primary reason why the governments are moving from regulation of data - to protecting data and protecting the data subjects or citizens, and India is no exception to this. There is no global privacy regulation, a; therefore, governments find it difficult to regulate it due to jurisdictional conflict regarding how states treat data. In the past, states have enacted data protection regimes, for example, GDPR in Europe, California Consumer Privacy Act in California and PIPL in China. India is rather late to the party as the Indian Parliament is currently discussing its data protection bill PDPB.

As technology advances and regulations are implemented, India has been on everyone's radar. This is because India is perceived as the synonym for the IT outsourcing industry. In the year 2020, the IT BMP industry of India alone contributed to 8 per cent of total GDP. In addition, India contributes 38 per cent of the global market share of the IT sourcing industry (NASSCOM). Many big companies prefer to outsource to India due to various reasons, such

---

[1] E. Kiesow Cortez, *Data Protection Around the World, Information Technology and Law Series 33*, 2021 Pg. 269

[2] M. Zalnieriute, *Data Transfers after Schrems II The EU UD Disagreements over Data Privacy and National Security* 2022 Pg. 3

[3] Ibid2 Pg. 4

[4] Available https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682

as quality of services, low cost of development, lower wages and many more. According to Software Park of India, software exports by the IT companies connected to it stood at US$ 16.29 billion in the first quarter of the year.

Against this context, through this thesis, I try to examine Indian laws and analyze whether they provide a sufficient level of protection of data. In doing so, I conduct a comparative analysis with the GDPR. I compare it to the GDPR because European developments have always influenced India in terms of legislation[5]. Although the existing laws and legislation do not provide an adequate level compared to the GDPR, there is still scope. The Supreme Court of India recently declared that India's 'right to privacy is a fundamental right'. In addition, the Indian parliament has initiated a bill regarding data protection. This could be a game-changer and strengthen the privacy framework in India. In the current thesis, I examine India's data protection framework and answer whether it provides a sufficient level of protection for the GDPR.

This thesis was initiated around March 2022 and as per the current news in March, it was stated that the Personal Data Protection of Bill will be passed during the second half of 2022 (September). Furthermore, a news was published on third of august (a few days before the submission) of the thesis, that the Bill has been withdrawn.[6] Nonetheless, it was stated that the new bill will not have many deviations from the Bill of 2019 and yet I suggest that the thesis will still be relevant. The new bill will be an updated and more internationalized version of the 2019 Bill. Therefore, the analysis done in the thesis would be relevant in the future.

Structure of the thesis & Research Questions

The thesis title uses the phrase, ‘data protection in the world's largest democracy. Is it a paradox?' this was the question one of my seniors asked during my traineeship. He argued that it was incomprehensible to have GDPR-style legislation in India, a country with numerous citizens and a lack of the rule of law. That was why I chose data privacy laws in India and data transfers to India as this Master Thesis topic. I realized the importance of data transfers to India when I was a trainee at PricewaterhouseCoopers Oslo. While I was doing extensive research

[5] See for example, Indian Competition Act, 2002 and Indian Companies Act 2013.

[6] Available Govt withdraws Data Protection Bill, 2021, will present new legislation | Business Standard News (business-standard.com)

on GDPR and data transfers to India, I understood that there is no clear and well-defined understanding of the laws and the common law system in India. Therefore, this master thesis is an attempt to explore the topic of data privacy in India'. In doing so, the research follows a theoretical and comparative approach. Although the central question of the thesis remains whether India has and existing or is on its way to replicate the GDPR that can ease business or give India a chance to obtain an adequate decision by the European Union.

The research seeks to address the following five questions that are answered in five different chapters:

The thesis is divided into five Chapters:

Chapter 1 is the starting point of this thesis that sets the background. Chapter 1, named 'Outsourcing', is the main reason I dive into data privacy and take a closer perspective. Therefore, in Chapter 1, I write about outsourcing, its history and why India has become an ideal place for outsourcing by various international entities. The Chapter also includes the legal and political reasons why outsourcing to India is so popular; therefore, I look at the tax benefits and central and federal government policies that promote outsourcing. Towards the end of the first Chapter, I discuss the potential threats of outsourcing to India. The first research question emerges in Chapter I: What factors play a role in India being an outsourcing hotspot? Therefore, at the end of the Chapter, I will be able to answer the question in the light of general, legal, and political reasons.

Chapter II, named 'is privacy dead', offers an academic approach, introduces topics such as data privacy and privacy laws, and explains general terms regarding data privacy. This Chapter further narrates the history of data privacy in Europe and looks at the GDPR and the game-changer Schrems II case law. Furthermore, the Chapter explains why data privacy is vital in a democratic state. The changes in data privacy transfers from Europe to the rest of the world are also looked at through the lens of the European Data Protection Board. Therefore, the second research question that emerges in this Chapter is: What is data privacy, and why is it essential in a democracy? Secondly, how has Schrems II influenced cross-border transfers from Europe to the rest of the world and what has the European Data Protection Board done to make data transfers strict?

In Chapter III, I introduce the legal regime relating to data protection and informational technology in India. In doing so, I analyze the historical context and the current and future proposals in light of the surveillance laws in India. In doing so, I refer to the European Data Protection Board report that was published in November 2021. The question in chapter III is what the surveillance laws in India are and how they affect cross border transfers. Are there

any Indian laws that allow the Indian government to access foreign data? We further answer the question whether India despite having signed various international treaties, follows a serious approach and respects fundamental rights of citizens and non-citizens.

Chapter IV relates to Chapter III as we analyze the main differences between the GDPR and the anticipated Protection of Personal Data Bill. Therefore, in doing so, I compare provisions of the upcoming Act and the GDPR and try to answer general questions such as what the similarities and differences are. For example, general principles, legal basis for processing, conditions under which sensitive data can be processed, data localization etc. As per 3rd August. 2022 the Bill has been withdrawn yet I believe it is still necessary to compare the two legislations and understand as to what was lacking and what shall be amended and added in the new bill. The new bill that will be passed in the month of February next year, will take its base from the Protection of Personal Data Bill, 2019. Therefore, it still holds relevance in the analysis.

Chapter V is the last chapter of this master thesis and tries to look at the future of India and data protection in the country. Therefore, we answer the question, whether the upcoming bill and the Puttaswamy judgment strengthen the data privacy framework in India. In this part, I also had a chance to conduct an interview and hear thoughts of a data privacy activist from India. Together with research and interview, we conclude whether the Indian government tackles issues such as human rights, privacy, and rule of law with utmost significance or not.

Demarcations

This master thesis attempts to look at the data privacy legal framework in India. In doing so, I have attempted to analyze the Indian laws in the light of European Union Guidelines, laws, and statutes. This thesis does not look deeply into the Indian legislative or judicial. Moreover, an interview was conducted in chapter V, which shall not be regarded as legal advice.

Literature review

There is significant research and works that address data privacy and the legislation that revolves around it. However, there are different approaches taken by authors, scholars and states. For example, how data privacy is perceived in Europe is completely different from how it is perceived in India. However, the book by Lee Bygrave ‘Data Privacy Law: An International Perspective’ gives an interesting and thorough knowledge about data privacy laws across borders. It is also interesting to rely on this literature because it builds on various codes and principles, such as OECD, Convention 108, and EU General Directive.[7]

Although when it comes to the works and research about Indian law, I refer to various Indian journals, articles and books that give a thorough look into Indian laws. However, an excellent European perspective of the Indian laws is presented by the European Data Protection Board report dated November 2021.[8] The report carried out by the EDPB does not have a binding effect and is only a study that can be relied on for informative purposes. Therefore, most of the research is based on diving deep into the legislations in India.

[7] B. Patricia. *Book Review*: *Data privacy law: an international perspective, by Lee Bygrave, Oxford, UK, Oxford University Press, 2014, XXIX, ISBN 978-0-19-967555-5. Information & Communications Technology Law*. 2015 Pg. 3

Chapter 1 Outsourcing

I lost my job, my car, and my house, when ten thousand miles away some guy clicked on a mouse[..] - Billy Bragg

(Songwriter)

The contemporary connotation of outsourcing implies getting the work done outside of an office, location, or nation for miscellaneous reasons. Outsourcing is not a recent concept, but it dates to the 1600s when the British employed people in Antigua to process sugar.[9] Historically speaking, outsourcing is embedded with the growth of business enterprises that the world witnessed in the second half of the 19th century.[10]To quote Tim Hindle "outsourcing has been increasing since the second world war, and especially rapidly in the 1990s. According to one estimate, in 1946 only 20 per cent of a typical American manufacturing company's value-added in production and operation came from outside sources; 50 years later, the proportion had tripled to 60 per cent."[11] Likewise, it has recently attained popularity due to the market's availability of efficient manual labour. Therefore, it has evolved into an essential source of employability, enabling governments to release some part of the burden, and creating across-the-board jobs. This clearly has benefited various countries, and India is one of them.

1.1 History of Outsourcing to India

In the 20th century, the world witnessed a flourishing technological and communications innovation industry. It was nearly like history was repeating itself, as old trends emerged and there was a significant change in society. In the last 25 years, as technology evolved, so did outsourcing. A major consultancy firm, for example, Arthur Andersen, invented remote

[8] European Data Protection Board *Government access to data in third countries*, November 2021. Available legalstudy_on_government_access_0.pdf (europa.eu)

[9] B. Vagadia *Outsourcing to India Legal Handbook* 2nd edition Springer 2007 Page 1

[10] A Gonzales & Others *Outsourcing: Present, Past and Future* 2004 Pg. 1 Available Dorwin.pdf (washington.edu)

[11] Ibid 9 Pg. 67

management systems.[12] Andersen promised that the services provided to the customers were of high quality and this was doing through Service Level Agreements or SLAs. One of the main reasons why the customers liked the services was due to constant availability of their network and services. The Indian government, which was initially based on a socialistic and protectionist model, initiated a liberalization program in the early 1990s.[13] Once the liberalization and globalization commenced, there was no looking back for the Indian Government. However, one would still pose a question as to 'Why India?'. There is a myriad of reasons why India became a favored destination, but the most common factor was education. India recognized the significance of education, and the state played a fundamental role in facilitating education and building universities. As of 2022, there are about forty thousand plus technical universities in India.[14]

The massive success behind this is the initiatives taken by the government. The Indian government set up various commissions, and one such example is the University Grants Commission established in 1952. This commission has played an essential role in ensuring good quality of education by looking over the curriculum and ensuring that the education is modern and up to date. I agree with the author that the Indian government was aware of the importance of technology, therefore emphasizing productivity by emphasizing work experience, vocational studies, scientific and technological education, and research. Therefore, concluding India as a world player in outsourcing. [15]

Often referred to as offshoring, but when it comes to India both the terms are used. [16] In India there are mainly two types of outsourcing:

1. Information Technology Outsourcing or ITO (related to all IT functions, such as software development, hosting, applications, or infrastructure)
2. Business Process Outsourcing BPO (where a third party is hired as an entire function, such as, HR, payrolls, customer care etc.)

There are various reasons why countries choose to outsource to India. Dr. Bharat Vagadia argues that companies outsource to India due to various reasons such as:

1. Focus on core functions of their own company

[12] Ibid 10, Pg. 3

[13] Ibid 10, Pg. 14

[14] Available https://www.statista.com/statistics/1102329/india-number-of-colleges/

[15] Ibid 10, Pg. 4

[16] Ibid 9, Pg. 1

2. Access to cheaper and specialist skills to match the competition
3. Reduction of costs through new and innovative technologies.

It is generally said that India is an ideal destination for outsourcing and one such example can be taken from the Virgin Group which outsourced its business functions to India and South Africa and cut down its costs by 15%. Another example, the author states is the Norwich Union and insurance company that outsourced approximately 500 IT jobs to achieve flexibility in their IT base.[17] One of the most famous IT companies from India known as The Tata Consultancy Services presented a report stating their support to the biggest banks across Europe.[18]

1.2 Legal and Political Reasons

It is not only just the economic and technical reasons why countries choose India as an outsourcing destination but also political and legal reasons. The Indian government itself has taken various initiatives to promote the growth of IT industries.[19] The government policies have created a legal and political environment that is preferable by various companies. India offers a tax friendly environment; it has a separate Ministry of Technology that investigates the matters related to IT. The central government established a task force to develop a high-class knowledge based outsourcing industry allowing duty free imports of capital goods and providing tax exemption on export of IT services.

Both the central and federal government have focused on IT and therefore made it an integral part of the agendas. For example, Software Technology Parks have been set up in various big cities of India which created more opportunities.[20] Moreover, very recently the Indian Government led by Narendra Modi, has initiated the Digital India plan. The plan aims to create a digital infrastructure that enables participate of every Indian citizen despite their background.

---

[17] Ibid 10, Pg. 4

[18] Available https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/about-us/analystreport/TCS-Leaders-Ovum-Decision-Matrix-Selecting-Core-Banking-System-in-European-Market-2016%E2%80%9317.pdf

[19]Available Other Projects & Initiatives | Ministry of Electronics and Information Technology, Government of India (meity.gov.in)

[20] Available https://stpi.in/en/about-stpi#:~:text=The%20first%20historic%20event%20that,Software%20Technology%20Parks%20of%20India.

Secondly, it aims to integrate across government departments that always ensure availability of services.[21]

The central government also has various tax incentives to attract multinational companies. An Indian domestic company that has its entire set up in India is bound to pay around 37 percent of tax to the government. Whereas a non-Indian company has to pay around 48 percent taxes and an additional minimum alternate tax of 8 percent. Therefore, companies prefer setting uo their offices in India. In addition, there are various tax reforms for IT industries, for instance, a 10-year tax break to establishments that are engaged in developing and maintaining the infrastructure. It also exempts them from paying 10-year tax power tax and a tax break is given to companies that set up their ventures in industrial parks and special economic zones in India. There are also state level incentives that offer rebates on the cost of land and lease of land.

With the growth of outsourcing, grew growth of cybercrimes, issues with law enforcement and compliance. It was in the year 2000 that the Indian parliament passed the Information Technology Bill that was later enacted in 2000. The Act helped in bringing the e commerce under the purview of strict rules and regulations to combat cybercrime. It also eases businesses as it allows the recognition of electronic contracts. It is not just the technology act whereas amendments have been made to the Indian Evidence Act and the Indian Penal code that cover the scope of cybercrimes.[22]

1.3 Potential risks and drawbacks with outsourcing

Despite India being an ideal destination for outsourcing, some developments show that there are various risks and drawbacks involved. An interesting article by Sarah Hilley titled as ‘when you outsource to India, where does your data go’. In the article, she states that many Indian IT companies that provide the world with services further outsource the services to countries such as Sudan, Iran and Bulgaria. Therefore, this is one aspect that increases the risk. There have been warnings given by risk management professionals to stop and check that the service provider in India is obliging by the contractual obligations and not outsourcing their services. She argues that one of the main reasons behind this is as India is facing labour shortage and lack of proper infrastructure. Due to the burden and the need to cope with the burden, tit has

[21] Available https://www.opindia.com/2019/03/digital-india-how-the-modi-govt-took-massive-strides-in-turning-india-into-a-digitally-empowered-economy/

[22] Ibid 10. Pg. 16

indeed, been in practice that India has outsourced its services beyond.[23] Therefore, it is very important to perform a due diligence on services, contracts and follow up compliance.

Moreover, other countries like the Philippines have also stepped in the competition and therefore making India a less attractive destination.[24] There have also been instances of public backlash from the US and European Union, as thousands of jobs have been eliminated from their own market and outsourced to India.[25] Recent developments also show that one of the biggest threats is to the data privacy of individuals. India does not have a legislation that provides for a sufficient protection of data and therefore, where the data flows can be a big threat. This shall be discussed in the succeeding answers.

Chapter 2 Is Privacy dead?

A simple google search describes the term 'privacy' as a state in which one is not observed or disturbed by other people'. It sounds easy, and one feels secure and shielded from any outside elements, but this might not be applicable when one is engrossed with technology and digital devices. For example, someone who comes back home from work uses devices such as Google Home or Alexa to switch on the lights, opens Facebook to connect with her friends, and uses dating apps to meet new people over the weekend. She might think she is safe and in a state of being free from interference, but she would not know that she can be heard with one click. She is oblivious to the fact that someone retains all the information about her without her knowing. The Internet is perceived as a threat to privacy yet is used in ways that expose our private lives on a daily basis. In the academic literature, this is used as a 'privacy paradox.'[26] What leads to this modernistic term ‘privacy paradox’ consists of factors such as:

i.) people presuming that their online life is safe and private,

ii.) The characteristic of the internet at a mechanical level is in proportion with privacy and

iii.) One’s expectation of privacy does not form of a privileged communication.[27]

---

[23] S. Hilley, *when you outsource to India, where does your data go: Not where you think* Computer Fraud & Security. Issue 6, 2004 Pg. 1 Available https://www.sciencedirect.com/science/article/pii/S1361372304000703

[24] Ibid 10 Pg.19

[25] Ibid 10 Pg. 19

[26] M Ziegele, O Quiring *Privacy in Social Network Sites 2011 Pg. 61 Available* https://doi-org.ezproxy.uio.no/10.1007/978-3-642-21521-6_13

[27] Ibid 25 Pg. 3

This also poses a question in my mind: how did we come so far? What went wrong, and what went right? The answer behind this lies in the three vicissitudes society witnessed. Poullet argues that the development of information technology can be traced chronologically along three aspects. To begin with, Moore's law, which in simple terms is understood as the 'growth of computers.'[28] A period when the user terminals and communication infrastructure changed rapidly. The aftermath of the internet revolution comes second in chronological order. All the networks were converged around a single interoperable platform and the appearance of semantic web or Web 2.0. These were two approaches that targeted the improvement of the world wide web through optimization of mechanisms for sharing information and resources[29]. Thirdly, the stage that we are still in is the emergence of artificial intelligence, which combines technology and network and penetrates our daily lives, the places we visit, the things we do, and the way we interact with society.[30]

2.1 Data privacy law and who does it apply to?

It is not only necessary to regulate data privacy but also necessary to regulate it in various stages. Bygrave explains that data privacy law regulates data processing stages and how data is gathered, registered, stored, exploited, and even disseminated. However, one may ask, what types of data are we referring to? Does it apply to all bits and bytes of data? Data Privacy law only applies to personal data that can be related to an identifiable person. The General Data Protection Regulation defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'(Article 4 (1)). On the same notion, the California Consumer Privacy Act uses the term personal information instead of personal data and defines it as 'information that can identify, relate to, can describe and is reasonably capable of being associated with, or could reasonably

---

[28] G.E Moore *Moores Law states that the number of transistors on an affordable CPU would double about every 18 months.* Available https://www.umsl.edu/~siegelj/information_theory/projects/Bajramovic/www.umsl.edu/_abdcf/Cs4890/link1.html

[29] Definition taken from the abstract - The open knowledge society. A computer Science and Information Systems Manifesto available https://doi.org/10.1007/978-3-540-87783-7_51

[30] Y. Poullet, *Data Protection legislation: What is at stake for our society and democracy?* Computer Law & Security Review 25, 2009 Pg. 217

be linked directly or indirectly, with a particular consumer or household.[31] Both the legislations provide a similar definition, but one finds differences. For example, GDPR covers publicly available data whereas the CCPA does not apply to information that is publicly available. Secondly, the GDPR prohibits the processing of sensitive data that relates to a person's political opinion, sexual orientation, health etc. It can only be processed if one of the legal basis provided in Article 9 applies. Therefore, making it extremely hard for a company to process such data. On the other hand, the CCPA does not separately define or categorize sensitive data or special categories of data. Although both the legislations term biometric data as personal data. The CCPA does not include medical data, whereas the GDPR is extremely keen on protecting one's health data. Various jurisdictions have a different way of defining and treating data. What one jurisdiction considers as sensitive data might not be considered sensitive in another jurisdiction.

2.3 Why is it important to have privacy in a democracy?

Democracy as a political ideology is based on transparency, rule of law and a state that is for the people, by the people and of the people. The Greek philosopher Aristotle explained the division between the public sphere of the political affairs (polis) and the personal sphere of human life (*oikos*). This dichotomy provides 'a confidential zone on behalf of the citizen'[32] In addition, John Stuart Mill, in his essay 'On Liberty 1859' elucidated the importance of citizen liberty from government authority. Mill stated that the oppression of the citizens by authoritative bodies can only be achieved by civil rights such as right to privacy, free speech, assembly, and expression[33]. Even in the recent times, authors and scholars define the concept of privacy based on concepts of privacy laid down by scholars such Warren, Brandeis[34] and Thomas Cooley[35]. The right to privacy, coupled with modern times, has posed various challenges in defining the term and understanding its importance in a democratic state. It is not just the law that dictates our lives but also technology. Moreover, technology is growing and transforming, making the future of privacy look dark. The author states that the demise of

---

[31] California Consumer Privacy Act 1798.140 (o) 1 Available https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[32] M. C. James, "*A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe",* Connecticut Journal of International Law Vol. 29, Issue 2, 2014 Pg. 261

[33] John S. Mill, *'On Liberty'*, Batoche Books 1859 Page 13.

[34] Warren and Brandeis, "*The Right to Privacy", Harvard Law Review*, Vol.4, No. 5 1890, Pg. 193

[35] Thomas Cooley defined the right to be alone in Treatise on the Law of Torts 1888, 2nd edition

privacy is a result of an arms race in communication tools and data mining capabilities. [36] He further argues that this is indeed due to the progression of Moore's law.[37] This was indeed true, but now technology is transforming at an even faster speed, and the reason is digital technology is now cheaper, easily accessible and distributed at a large scale. Therefore, posing a threat to privacy as the hassle of protecting privacy is growing as well. [38] There are more than 1.5 billion people who use email services. Technology has already combined mobile phones, computers, and televisions. There is indeed a lot of information circulating around us and about us. The way information is collected in multiple ways, including CCTV cameras, mobile apps, social media, and various other means. Moreover, the way this information is saved can also be done in many ways that a normal user is unaware of. The information that we put online ourselves through social media, traffic, cookies, tracking information, keyword searches and the list go on.[39] Another question that comes to one's mind is who precisely processes this information about us? Typically, one would believe it's their employer, university, or the bank where they have an account. These might not be the only ones processing our information. It could be a website we went on, social media apps and their third parties. Presumably, even an app that you no longer use anymore but consented to without reading the terms and conditions. These do not display the components of a democratic liberal state. I draw reference to the decision o the German court regarding the 1983 census. Whereby the German court laid stress on the protection of personal data that was collected through the census. According to the judges, the existing law had shortcomings and omissions as no explicit definition, objective or transparent methodology was observed regarding the personal data of German citizens. Therefore, concluding that the deficiencies constituted an attack on human dignity and the proper development of the person.[40]

Article 8 of the Universal Declaration of Human Rights safeguards the right to respect for one's private and family life. The notion of the right to a private life is enshrined in national and local laws as well. For example, in India, Article 21 is the soul of the Indian Constitution. It states that 'no person shall be deprived of his or her personal life or personal liberty except according

---

[36] F. DeBrabander. *Life after Privacy: Reclaiming Democracy in a Surveillance Society*. Cambridge: Cambridge University Press 2020

[37] Ibid 27

[38] Ibid 35 Pg. 58

[39] Ibid 29 Pg. 2

[40] Available https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

to a procedure established by law. This is a right that is not only applicable to the citizens but to every person who is in India, including travelers and foreign diplomats. The Indian constitution was drafted in 1950, a period when technology was not developed, and no one could have anticipated that technology would grow - or outgrow us. After 1990, when India became a part of the globalization and liberalization movement, multifarious threats to the democratic state were posed due to diverse reasons, such as overpopulation and lack of legislation surrounding technology. Consequently, the right to data privacy never was scrutinized until recently. In the year 2017, the Supreme Court of India, in a 9-judge bench, declared the 'right to privacy as a fundamental right'. The judgment will be further explained in detail in chapter 3.

To conclude, I articulate that a democratic state and its values emanate from freedom and liberty. In the light of the preceding assertions made above, I conclude that the right to a private life is indeed an essence of democracy. A state without freedom of expression, constant surveillance and lack of personal space cannot be termed a 'democracy'. Moreover, currently in modern times, technology is so intertwined with our lives that it makes it even more necessary to respect privacy not only offline but also online. Therefore, it is the utmost duty that technology and data should be used in such ways that it benefits society and does not take away the essence of democracy and the rule of law. If technology offers risks, it can also provide us with solutions. Therefore, agreeing with the author's arguments and emphasis laid on French law (1978) that '*Information technology should be at the service of every citizen. Its development shall take place in the context of international cooperation. It shall not violate human identity, human rights, privacy, or individual or public liberties*[41].'Therefore, data privacy is extremely important for individuals, their lifestyles, and a liberal democracy.[42]

2.4 Data privacy in Europe

As mentioned in the introduction, I draw my reference to the GDPR, a European legislation on data privacy as it has been a guiding principle for not only the upcoming Indian data privacy Act but to many States across the globe.[43] The GDPR was adopted in the year 2016 to replace

[41] Ibid 29 Page 223

[42] V. Boehme Nebler *Privacy: a matter of democracy. Why democracy needs privacy and data protection* International Data Privacy Law Volume 3 No. 3 2016 Pg. 226

[43] The Joint Parliamentary Committee, India in its recommendations refers to the GDPR in various areas. Available http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

the existing Data Protection Directive 1995. It was the result of many negotiations, amendments and took around 4 years to be finalized as a regulation.[44] The aim behind the regulation was to regain the trust of the people across Europe and boost the digital economy.[45] It laid down stringent rules for companies, organizations and other bodies that were dealing with personal data of European citizens. It laid down organizational requirements for the entities such as recording of processing activities, appointment of a data protection officer, conducting privacy threshold assessments and data protection impact assessment while using new technologies. It initiated new concepts such as data protection by design and by default, data subject rights and implementation of technical and organizational measures while processing data. Moreover, it obligated entities to provide with a legal basis while processing personal data of data subjects. Therefore, overall creating a strict regulation that left various companies in a chaos and therefore being non complaint with the new regulation.[46]

2.5 Schrems II – Game Changer – Brief Background

Schrems II, known popularly as the abbreviate for the case Data Protection Commissioner v. Facebook Ireland Limited Maximillian Schrems (C-311/18), is a case that was initiated by Max Schrems, an Austrian lawyer and the founder of NYOB (none of your business).

He first gained popularity when the CJEU ruled Safe harbor invalid.[47] The safe harbor mechanism was relied on to transfer data from Europe to the US. The background of the first ruling by the CJEU stems from a complaint made by Max to the Irish Data Protection Authority asking them to investigate, as he believed that his Facebook data was transferred from Ireland to the US. He argued this in light of the Snowden revelations about a data collection program by the NSA called PRISM. He further argued that the US law practices did not provide adequate protection to his personal data and the data of other European citizens. The Data Protection Authority rejected this complaint, and they stated that the transfer relied on the EU US Safe harbor mechanism. By the time this case was appealed to the CJEU for a decision. The CJEU concluded with the following

---

[44] P Voight & A. von dem Bussche The EU General Data Protection Regulation (GDPR) A practical Guide 1st edition, Springer 2017 Pg. 2

[45] Ibid 43 Pg. 2

[46] Available https://www.ciodive.com/news/data-privacy-CCPA-GDPR-fines/572077/

[47] Available https://www.dataguidance.com/resource/definitive-guide-schrems-ii#supplementary%20measures

1. If an adequacy decision exists with a country, it does not reduce a citizen right to claim an examination by the Data Protection Authority.
2. Held that the Safe Harbour is insufficient and does not provide the same level of protection to the EU citizens.[48]

Initially, many businesses across Europe and US relied on the Privacy Shield to transfer data from the European Union to the US. The Privacy Shield entrusted with safeguards and protection for EU/EEA companies to transfer data legally to US-based companies that were listed in the Privacy Shield list. The companies were admitted to the list administered by the US department of commerce, and the US Federal Trade Commission monitored the compliance.

By declaring the Safe Harbor invalid, the Court emphasized the need to protect the fundamental rights of the citizens. The Court also emphasized that the level of protection shall be construed together with the right to privacy as laid down by the Charter of Fundamental Rights, which includes the right to privacy and judicial remedies and provides national data protection authorities with supervisory powers.

Following the Schrems I judgment, Facebook relied on SCC or standard contractual clauses to transfer data. Max reformulated his complaint and articulated that the SCCs were insufficient as the US Surveillance programs infringed his fundamental rights. It was in July 2020 that the CJEU finally declared that:

1. The Court made a reference to Article 2-4 of the GDPR and stated that it applies to the transfer of personal data for commercial purposes between a member state and an economic operator that is established in a third country.[49] Moreover, the Court held that processing of personal data for national security did not invalidate the application of the GDPR.[50]

2. The Court confirmed the use of standard contractual clauses (SCCs) but laid down stricter measures if the company was to rely on them. The Court highlighted that transfer could only

[48] S. Monteleone, *Members Research Service European Parliamentary Research Service* Available https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/569050/EPRS_ATA(2015)569050_EN.pdf

[49] CJEU C 311/18 – Data Protection Commissioner V. Facebook Ireland Limited and Maximillian Schrems II Judgment Paragraph 89

[50] Ibid 49 Paragraph 89

happen if the provisions of the contract provided 'essentially equivalent' protection for personal data transfers[51]

3.Therefore, the Court finally found that Privacy Shield was invalid as it was still not safe from the purview of surveillance, there was lack of redressal mechanism for citizens and a lack of authority or independence of ombudsperson.[52]

2.6 How has it changed data transfers outside of Europe?

I am very happy about the judgment. It seems the Court has followed us in all aspects. This is a total blow to the Irish DPC and Facebook. The US will have to seriously change their surveillance laws, if US companies want to continue to play a major role on the EU market.

Max Schrems, 2020[53]

The rulings of the CJEU did not only affect the transfer from EU to US, but it brought along every 'third country' under its purview, impacting transatlantic economy and commerce, data sharing frameworks in law enforcement, and international data transfers.[54] A report presented by NASSCOM provides a very brief summary of how data transfers have changed after Schrems II. In the report they state the following:

Firstly, one of the biggest changes made was the guidance to use SCCs. The court held that the SCCs are valid, but they are only there to provide contractual guarantees. As the public authorities are not binding to the SCCs therefore, they do not bind them to follow the contract. Therefore, requiring doing an assessment of the law of the third country.

Secondly, the CJEU suggested that the organizations can transfer the data if no adequacy decision exists, but it is necessary to provide appropriate safeguards, rights and effective legal remedies. The Court used the term 'essentially equivalent' while referring to protection of data subject rights.

---

[51] Ibid 49 Paragraph 105

[52] Ibid 49 Paragraph 199

[53] CJEU Judgment - First Statement, NOYB (July 16, 2020), https://noyb.eu/en/cjeu [https://perma.cc/G3Y3-VWJV] (archived Oct. 20, 2021).

[54] Monika Zalnieriute Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security January 2022Page 37

Thirdly, the EU data protection authority should suspend all transfers that do not provide adequate safeguards. Moreover, if the organization fails to comply with the regulation, the data should be returned or destroyed, and the data subjects shall receive compensation for the damages.[55]

The aftermath of Schrems II was such that practitioners and advisors around the world tried to assess the impact of transfers to their countries. Although the radar was over EU US transfers but there were concerns about other countries as well. The data exporters were obligated to take supplementary measures and assess every case according to the laws in the country, the practice and adopt additional safeguards where required.

2.7 What are the EDPB essential guarantees

Schrems II and its impact has been discussed thoroughly in the previous chapter. It was concluded that Schrems II was a game changer for privacy, data, and surveillance laws across the globe. Therefore, following the judgment, the European Data Protection Board (EDPB) assembled in the working party 29 and drafted the EU essential guarantees. There are guidelines that are laid down by the EDPB in order to tighten data transfers from Europe to a third country. These steps were taken by them to enhance privacy and protect the personal data from surveillance laws in the third country.

The essential guarantees are also linked to various other treaties that the EU is a part of, for example, articles 7[56], 8[57] and 47[58] of the charter of fundamental rights of the EU Charter of Fundamental Rights, and Article 8 of the European Convention on Human rights that deal with surveillance issues[59]

---

[55] NASSCOM Implications of Schrems II on EU India Data Transfers August 2021. Available https://nasscom.in/sites/default/files/202108_NASSCOM_Schrems_II_Study.pdf

[56] Article 7 *Respect for private and family life.* Available https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life#:~:text=EU%20Charter%20of%20Fundamental%20Rights,-Previous%20title&text=Everyone%20has%20the%20right%20to,family%20life%2C%20home%20and%20communications

[57] Article 8 *Protection of personal data.* Available https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life#:~:text=EU%20Charter%20of%20Fundamental%20Rights,-Previous%20title&text=Everyone%20has%20the%20right%20to,family%20life%2C%20home%20and%20communications

[58] Article 47 *Right to an effective remedy and to a fair trial* Available https://fra.europa.eu/en/eu-charter/article/47-right-effective-remedy-and-fair-trial

[59] European Data Protection Board Recommendations 02/2020 on the European Essential Guarantees for surveillance measures 10 November 2020 Pg. 4

The Schrems II judgment serves as an example while assessing third countries' surveillance laws. The EDPB stated that it is indeed the final verdict of the court to decide whether surveillance laws interference can be justified while weighing it against fundamental rights, but if there is no judgment providing any help, then the data protection authority must assess the individual case. Therefore, the EDPB updated the guarantees in order to provide more information for examining the elements of surveillance laws in the third country.

Therefore, these essential guarantees form a part of the overall assessment to determine whether the third country provides the same level of protection equivalent to the ones guaranteed under EU law. In addition, they need to be read in light of articles 46 and 46 of the GDPR.

2.7.1 Basis of these guarantees

The European Union's general principles are fundamental rights enshrined in the European Convention on Human Rights. The Court also corroborated in the present case that "the fundamental rights enshrined in the European Convention on Human rights are also confirmed by Article 6(3) of the Treaty of the European Union. Moreover, Article 52(3) of the Charter provides that the rights contained in the Charter, which correspond to rights guaranteed by the ECHR and have the same meaning and scope as laid down in the convention. Moreover, the Court held that the interpretation of the EU laws and their legality should be seen in the light of fundamental rights guaranteed by the Charter. The Court emphasised that in the absence of an express reference to the national law of the Member states, their interpretation cannot be considered on the sole basis of the national law.[60]

2.7.2 Protection of fundamental rights

Articles 7 and 8 of the Charter lay down right to personal life, private life etc. article 8 furthermore sets conditions for processing of personal data lawfully and recognizes the right of access and rectification the data subjects have.

It was also held in the Schrems II judgment in paragraph 170-177 that when a fundamental right that is enshrined in article 7 is affected while processing the personal data, then the right to data protection is also affected. Therefore, this shall meet the requirements of data protection and fundamental rights. The court furthermore states that the fundamental rights enshrined are not absolute and therefore shall be considered in relation with the functions of the society.

[60] Ibid 49 Paragraphs 98, 99 and 100

Therefore, '*personal data may be processed for specific purposes and on the basis of the legitimate basis laid down by the law'*[61] *the court emphasised on the principle of proportionality and stated that '' in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must indicate in what circumstances, and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.*[62]

Therefore, the EU essential guarantees were developed and now they form a part of assessment along with other principles and statues and do not constitute an individual assessment. There are four European essential guarantees that apply to everyone irrespective of their nationality and they are as the following:

A. Processing should be based on clear, precise, and accessible rules
B. Necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated
C. An independent oversight mechanism should exist
D. Effective remedies need to be available to the individual[63]

Chapter 3 India

He thought of the telescreen with its never sleeping ear. They could spy upon you night and day, but if you kept your head, you could still outwit them. With all their cleverness, they had never mastered the secret of finding out what another human being was thinking.

George Orwell 1984I

In Chapter 2, under section 2.5, we explored the European essential guarantees laid down by

[61] Ibid 49 Paragraph 173

[62] Ibid 49 Schrems Judgment Paragraph 176

[63] Ibid 59 Pg. 8

the EDPB. This chapter is the lengthiest in the thesis and contains different sections. In section 3.1, I introduce India's legal framework for data protection and surveillance. This provides us with a general description of various statutes that were drafted that are related directly or indirectly to data protection or surveillance. In Section 3.2, I analyze the Indian data protection and legal surveillance framework against the EDPB essential guarantees discussed in the previous chapter. Section 3.2 further tries to answer whether there is a rule of law in India or a rule of politics. Therefore, by the end of the chapter, we will be able to answer whether India and the legal framework in India fit the EU's essential guarantees and provide equivalent protection to the citizens as European Union does. I also refer to the report published for the benefit of EDPB in November 2021, titled "government access to data in third countries."[64]

3.1 Legal framework in India relating to data protection and surveillance.

India, a socialist democratic state with a population of over 3 billion people, has miscellaneous laws across diverse sectors that deal with data indirectly. When referring to a data protection legal framework, it is stated that India is suffering from a temporary incapacity to deal with a fast-changing world. There are various grounds behind this. A highly populated country, lack of infrastructure, and state of affairs of the government are just to name a few examples.[65] Furthermore, the current legal framework does not fit the fast-changing technological developments. A closer look at the legal framework gives an overview that these are three main statutes that deal with data protection indirectly. Correspondingly, there are case laws, rules and the upcoming data protection bill that explains the data protection framework. This includes the following:

i. The Information Technology Act 2000 (IT Act) & the IT Rules drafted under the Act, also known as the SDPI Rules 201:

The IT Act, 2000, in its preamble, states that it was enacted to regulate electronic transactions and to safeguard the economic transaction online. Therefore, the act was enacted to give powers to the government and its agencies and not to protect the individuals from data misuse or risks associated with data manipulation or targeted advertisement. The scope of the IT Act is very narrow, and therefore, safeguarding the rights is a far-fetched idea.[66] In addition, it is

[64] EDPB Government access to data in third countries 2021, Available https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

[65] A. Srivastava *Data protection law in India: the search for goldilocks effect. European Data Protection Law Review* (EDPL), 5(3), 2019 Pg. 408-415.

[66] Ibid 65

also argued that the jurisdictional reach of the IT act is very narrow as it covers only body corporates and thereby does not mention State. The author further argues that the State is seen as a guardian of the fundamental rights of the citizens and suggests that the notion of data protection should also be directed toward the State. In the year 2008, there were amendments made to the IT Act, and surprisingly, the amended provisions also targeted corporate entities.[67]

In the year 2011, the SDPI rules were adopted under the IT Act, by the Ministry of Electronics and Information Technology (MIETY). The issues regarding data protection were adressed in the Rules, as various new legal notions and definitions were introduced. For example, terms such as cyber incidents were defined.[68] Therefore, this was seen as a positive step towards protection of data and misuse of data manipulation. Moreover, the term 'sensitive personal data' was defined which included – password, financial information such as card information, physical physiological issues, sexual orientation, medical history records and biometric records.[69] The author argues that the list is exhaustive and therefore, it does not leave room for other types of data mentioned. For example, data such as political beliefs, caste, gender, and genetic data are not included and thereby the Indian government kept this in mind while drafting the upcoming data protection bill, which will be discussed further.

ii. **The Telegraph Act 1885** and rules, setting forth the procedure and safeguards for interception of telecommunications: This Act, enacted in the year 1885 provides the central government with the authorization to establish and maintain the telegraphs. The term 'telegraph' is inclusive of all forms of telecommunications including wired and wireless equipment's that further includes data or voice.

iii. **Aadhar Act, 2016**: The Aadhar Act has a long history as the Aadhar scheme was launched by the government in 2010. A scheme that was to act like a simple tool to improve the public distribution scheme into the de facto national identity system.[70] In order to regulate these Aadhar cards the government in the year 2016 passed the controversial bill 'Aadhar Bill', in the parliament. After the Bill was passed, various entities demanded for the numbers in order to link them with bank accounts, subsidies and benefits. Over the years the government made

[67] After the amendment, Sections 66A and 66F were added that prescribed punishment for offences such as obscene electronic message transmission, identity theft, violation of privacy and cyber terrorism.

[68] Rule 2 (d) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 Available https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[69] Ibid 68

[70] Available https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html

it mandatory for applying for scholarships, higher educations, or mobile connections. The biggest revolt against the Aadhar act was the privacy issue. The opposition party argued that the biggest concern regarding the Act was mass surveillance of citizens. As this was supposed to be voluntary but later on it became compulsory. Furthermore, this led to the famous case law called ‘’Puttaswamy’, in the year 2017.

iv. **The Puttaswamy Judgment 2017**: If Schrems II was the game changer in Europe, the judgment of Puttaswamy is seen as the game changer for privacy in India. Although the right to privacy was long contested in India in various cases, it was never given a status of a fundamental right under the Constitution of India.[71] It was only recognized as a fundamental right when a 91-year-old retired judge, Puttaswamy, brought a case against the central government and posed the question ‘of whether the right to privacy could be guaranteed as a fundamental right.’ This was a question that arose in the year 2015 as well, whereas the constitutionality of the Aadhar Act (discussed above) was questioned. In 2015, the five-judge bench had refused to consider the right to privacy as a fundamental right, and therefore, it was referred to an even larger bench consisting of nine judges to pronounce the status of privacy rights under the Indian Constitution.[72]

Understanding the judgment: The 9-bench judgment runs into 547 pages. The Indian Central government argued that the concept of privacy is so ambiguous and, therefore, the court cannot recognize it as a juristic concept that it fails to withstand constitutional scrutiny.[73] Therefore, the Court took it upon itself to elucidate the concept of privacy in a democratic state. The judgment contains observations made by the judges, including a plurality opinion by Justice Chandrachud on behalf of four other judges. The remaining five judges provided a concurring opinion, and therefore, the plurality judgment cannot be regarded as the majority opinion. Moreover, the only binding and operative part of the judgment includes overruling previous judgments that stated that the right to privacy is not a fundamental right.[74] Therefore, concluding that the right to privacy is an integral part of article 21 of the Indian Constitution

---

[71] Available https://lawsisto.com/legalnewsread/ODk4Mg==/Judgement-Analysis-K-S-Puttaswamy-and-Ors-v-Union-of-India-2017-10-SCC-1

[72] V. Bhandari, A. Kak, S Parsheera, & F. Rahman *an Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. IndraStra Global*, 2017 1-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2

[73] Justice K.S. Puttaswamy and Anr Vs Union of India and Ors. 2019 1 SCC 1 2019 page 26 Available https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

[74] MP Sharma (1954) and Kharak Singh (1964) were overruled.

that provides the right to life and personal liberty. The Court stated that although our Constitution does not expressly declare the right to privacy as a fundamental right, this right forms an essential ingredient of personal liberty. In doing so, two judges relied on the observations made by Justice Frankfurter in Wolf v Colorado,[75]a case law that emphasizes the importance of security of one's privacy against arbitrary intrusion. [76] The Court furthermore maintained that a constitution of any country mirrors the aspirations and goals of the people of that country through representatives that are elected by the citizens themselves. There is a sense of trust entrusted to these elected people by the citizens, and therefore, they have the responsibility to draft a constitution that reflects the history and goals of the society. Therefore, it is the duty of the elected representatives to keep track of the changes and dynamics of the constitution. It is indeed necessary to keep in mind the evolution of technology and science and understand that they play an essential role in the modern world. Therefore, technological changes are to be kept in mind while drafting, amending, or interpreting the constitution, and the meaning of the constitution cannot be frozen to what it was decades ago.[77]

Courts take on the right to Privacy: Justice Chandrachud held concluded that life and personal liberty are inalienable rights and there cannot be separated from a dignified human existence. These rights form the foundational pillars of the Indian Constitution. He further elucidated that 'privacy has both a normative and descriptive function. At a normative level, privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty.''[78] The court concluded that informational privacy is an essential element of privacy and dangers to data privacy do not only originate from state actors but also non state actors. They commended the government to examine and draft a robust regime for data protection. It was further posited that creating a data protection framework in India requires a careful and sensitive balance between rights of the individuals and legitimate concerns of the state, such as national security, prevention and investigation of crimes, spreading of knowledge for research purposes, and preventing the dissipation of social welfare benefits.[79]

---

[75] Wolf V Colorado 1949 238 US 25

[76] Ibid 73 Pg. 16

[77] Available https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf page 263

[78] Ibid 73 Pg. 262

[79] Ibid 73 Pg. 265

Test for infringement of right to privacy: In the judgment, the court also laid down the test for infringement of the right to privacy. The Court stated that privacy under Article 21 (personal liberty) cannot be denied except through a procedure established by the law. The procedure established by law should be fair, reasonable, and just.[80] Therefore, in order to deny the right, Justice Chelameswar provided that in order to test the reasonableness, there shall be a menu of tests that can be used in privacy cases. If the right to privacy is violated in the context of an action of the state, it shall be tested under the reasonableness provided in Article 14 (right to equality) of the Constitution. Further, if the right to privacy is denied and influences freedom of speech (Article 19), therefore the reasonability has to fall under the conditions of Article 19. He further provides an example that if telephone tapping is to take place, which will intrude right to privacy and the right to expression. It shall be justifiable under conditions of article 19 (2) that enunciates 'fair, just and reasonable.' [81] Although the court concluded in favor of the right to privacy, yet it will have to analyze it per case-to-case basis. We will further discuss the case law while analyzing the data protection laws in India in the light of the EDPB Guarantees in Part 3.2

v. **The upcoming of Personal Data Protection Bill, 2019(withdrawn as per 3rd August 2022)**: As discussed earlier, the Puttaswamy judgment was one of the essential elements that led to the enactment of the Bill. Moreover, many other data driven business models in India raised the questions of privacy in the information world. There were instances where petitioners had challenged the data privacy policy of big companies such as WhatsApp at the Delhi High Court.[82] Although the court emphasized on having an opt out option yet there was no legislation dealing with data privacy. In the past there were efforts initiated to protect data privacy but some of them lapsed and some are still pending. Hereunder we can see the list of the initiatives takes by the government:

Date	Title of the Bill	Status
28.11.2014	The Personal Data Protection Bill, 2014	Pending
05.08.2016	Right to privacy of Personal Data Bill,2016	Lapsed

[80] The Supreme Court of India in various judgments emphasised on this, see for example, Bachan Singh V State of Punjab 1AIR 1980 SC 989

[81] Ibid 72

[82] Karmanya Singh Sareen v Union of India WP(C) 7663/2016 (Delhi High Court, India).

10.03.2017	Right to Privacy of Personal Data Bill, 2016	Pending
21.07.2017	Data Privacy Bill	Lapsed
03.082018	Data Privacy and Protection Bill, 2017	Lapsed
26.07.2019	Personal Data Protection Bill, 2019 (Including information privacy code)	Pending

(Source: Internet Freedom Foundation)

Therefore, it was emphasized by the Supreme Court that the central government initiate a data protection bill and the matter is taken seriously. Moreover, the GDPR and its prominence made various states re-shape their data protection regime and India was one of them. Therefore, a committee led by Justice Srikrishna was initiated, that discussed the enhancement of data protection in India. Thereby leading to the birth of Personal Data Protection Bill, 2019.

3.2 Indian Law in the light of EDPB Essential Guarantees.

3.2.1 Clear, precise, and accessible rules: Under the Indian law, it is the Code of Criminal Procedure, that stipulates the power to seek production of documents.[83] The provision does not set any further clarification and as does not meet the minimum requirement as per the essential guarantees. There is no mention of storage, rules for accessing personal data, precautions while communicating the data to others.

Under the Information Technology Act, section 69 lays down the power to issue directions for interception or monitoring or decryption of any information through any computer resource. Under the section both the central and state governments or their officials have the authority to access any possible computer source and collect information stored on in. The conditions that need to be met are '[…] necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any

[83] Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order. Available https://indiankanoon.org/doc/911085/

cognizable offence relating to above or for investigation of any offence.'[84] It furthermore, stipulates that any person who fails to assist shall be punished with imprisonment for a term that may extend to 7 years and shall also be liable to pay a fine. Under Section 69B of the Information Technology Act, the government is authorized to allow any agency to monitor and collect any traffic data and information from any computer, if there is a concern about national cyber security. The Report suggests that the provisions under the IT Act stipulate a certain degree of uncertainty around the decisions of the government based on the sections mentioned above.

The IT Act also orders intermediaries to provide a high degree of assistance to the government and its agencies. If an intermediary fails to comply with the direction of the government, can be imprisoned for seven years and liable to pay a hefty fine.[85]

Talking of the Aadhar Act, the constitutionality of it was challenged at the apex court of India, Supreme Court in the aforesaid judgment *Puttaswamy*. The petitioners challenged that it was infringing the fundamental right of private life of individuals. Although the court held the constitutionality of the Act but stated that it was not mandatory for non-welfare purposes and for the private sector. Therefore, in 2019 amendments were added to the Act[86]

3.2.2 Necessity and proportionality: Under the IT Act, there are provisions that lay down conditions for processing of personal data, in which, the state conduct is exempted. Moreover, the IT Rules 2011 also apply to body corporates and not to government bodies. Moreover, under the Interception Rules provided under the IT Act certain safeguards are provided to protect personal data against abuse of the data. For example, there are limits on the duration of the interception, there is a limit on the number of authorities that can order the interception. It also states that authority seeking information shall first consider acquiring the information from all means.[87]

Furthermore, this was also corroborated by the Supreme Court in Peoples Union for Civil Liberties V. Union of India, that there shall be certain guardrails against the governments use of surveillance and interception. The court designated safeguards to check the arbitrariness of an interception order, such as the orders can only be given by Home Secretary of the central

[84] Available https://indiankanoon.org/doc/1439440/

[85] Section 69A & 69B Information Technology Act, 2000

[86] Ibid 73

[87] The Information Technology (Procedure and Safeguards for interception and decryption of information) Rules, 2009 available https://indiankanoon.org/doc/30809273/

government or a state government. Moreover, the court emphasized that there shall be a review committee that may evaluate whether the interception order is compliant with laws.[88] Whether this is really in practice or not is a question that can be answered by taking some practical examples. For example, in the year 2020 a writ petition was filed before the Delhi High Court, challenging the operation and execution of the surveillance projects of the Indian government. The projects named CMS, NETRA and NATGRID seek to spy communications of the citizens were challenged on the grounds that they infringe righty to privacy of the citizens, aggregation of data that leads to profiling of individuals whereby hampering the free speech and freedom of expression of the citizens. The petition furthermore stated that these projects are against India's international commitments under the ICCPR, UDHR and other international obligations. They argued that these projects are against rule of law and against the principles laid down in the Puttaswamy judgment.

3.2.3 Independent oversight mechanism: Under the IT Act and the SDPI Rules, there is no mention of any independent oversight mechanism. This is one of the most important elements of the EDPB Guarantees. Moreover, under the Telegram Act, if an interception order is to be reviewed, it is done by the executive branch of the government which again is under the central government. Therefore, posing a threat to the independency of the authority. The report suggests that the government is responsible for making surveillance requests and therefore lack of a judicial or parliamentary oversight authority raises a concern.[89] Secondly, under the telegraph Rules 1951 the issue is similar, as there is no independent oversight mechanism and therefore it is emphasized repeatedly in the judgment that there is a need of an independent authority. Under the Aadhar Act, states that there shall be an independent oversight mechanism reviewing the government decisions. Furthermore, this article states that this oversight committee shall exist of a Cabinet Secretary, the Secretary to the government of India in the department of legal affairs and the secretary to the government in the department of electronics and information technology.[90]

---

[88] C. Ramachandran PUCL v Union of India Revisited: *Why India's Surveillance law must be redesigned for the digital age* 2014 Pg. 109

[89] NASSCOM *Implications of Schrems II on EU India Data Transfers* August 2021. Available https://nasscom.in/sites/default/files/202108_NASSCOM_Schrems_II_Study.pdf Pg. 22

[90] European Data Protection Board *Government access to data in third countries*, November 2021. Available legalstudy_on_government_access_0.pdf (europa.eu) Pg. 35

3.2.4 Effective remedies available to the data subjects and data privacy rights: Under the IT Act 2000 and the IT Rules 2011, it is the duty of the body corporate (the one that processes data), to have a privacy policy in place. Moreover, under the IT Rules it is necessary that the data subject should be informed about the purpose, scope and the name of the agency collecting their data.[91]Moreover, no sensitive data is allowed to be published without prior written electronic consent of the data subject.[92] More so, one does see some similarity between the data subject rights given by the GDPR and the IT act but when it comes to 'right to be forgotten', there is no mention of it in any laws. But looking a closer look at case laws tells us that women can have their information erased specially if there is information about sexual offences etc.[93]. There is no explicit legislation yet.
Under the Aadhar Act, 2016 we can see similarity with SDPI Rules 2011, especially when it comes to collection of data, purpose and who can the information be shared with (Section 3 of the Aadhar Act 2016). Furthermore, the data subject can access their information under the act, but biometric information is exempted from this and the information under the Act can only be disclosed in the case prior consent of the data subject is obtained.[94]

Many effective remedies and data subject rights can be found under various laws and statutes in India. A closer look at effective remedies tells us that it poses a constitutional question. Are there remedies found in the Indian constitution? Can one appeal the decision of the State? Lastly, is it available to non-Indian citizens? The answer to the above questions is a big yes. As per Article 32 of the Indian Constitution, the citizens have the right to remedial actions. Petitioners have the right to move to the supreme court if their fundamental right has been infringed. This is also known as the heart of the constitution.[95]

[91] Section 5(3) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

[92] P. Chowdhury, K Thayil, *Data Privacy in India*, 2021 Available https://www.mondaq.com/india/privacy/1005640/data-privacy-comparative-guide

[93] State of Punjab vs Gurmit Singh 1996 AIR 1393 SCC (2) 384

[94] Section 28 of the Aadhar Act, 2016 available https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

[95] Available https://www.jagranjosh.com/general-knowledge/article-32-of-indian-constitution-1605699265-1

3.3 Rule of law or rule of politics in India

India - a country with a long history, multiparty, parliamentary democracy with a bicameral legislature.[96] Under the constitution are twenty-nine states and seven union territories, with a high degree of autonomy and having the responsibility for law and order. The main source of legislature and rule of law is the Indian Constitution, which came into effect in the year 1950, few years after the independence from the British rule.[97] The Indian Constitution sets forth the rule of law for the country, which means that nothing is above the law. If any legislation fails to comply with the Constitution or is incompetent with the Constitution, it will be declared invalid.[98] Moreover, the Constitution lays down various other fundamental rights such as right to life (article 21), right to equality (article 14), freedom of speech (article 19). Furthermore, to strengthen the fundamental rights in India, a national human rights commission was established in 1993. India has also signed and ratified various international treaties such as the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights. Both the treaties acknowledge the right to privacy as a fundamental right.[99]

The Information Technology Act, 2000 does not lay down clear boundaries neither does it lay down a procedure for fair collection, storage, and accessibility rules. Moreover, the term 'intermediaries' has a broad definition and is inclusive of telecom service providers, social medias websites and apps, online marketing platforms, search engines and payment sites.[100] Therefore, this results to the Indian government having a lot of power over these private intermediaries to monitor and have access to personal data. The government accesses the data through private surveillance in the name of national and cyber security.[101] The question of jurisdictional scope also arises here, does this apply to Indian nationals or everyone? An amendment in 2008 to the IT Act, extended the criminal liability to any person, irrespective of their nationality. The only condition that needed to be met is ''such a conduct involves a computer, computer system or computer network located in India'[102]

---

[96] Available https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/india/

[97] Available https://www.india.gov.in/my-government/constitution-india#:~:text=The%20Republic%20is%20governed%20in,force%20on%2026th%20January%2C%201950.

[98] Article 13, The Constitution of India 1950 Available https://legislative.gov.in/sites/default/files/COI.pdf

[99] European Data Protection Board *Government access to data in third countries*, November 2021. Available legalstudy_on_government_access_0.pdf (europa.eu) Pg. 26

[100] Section 2 (w), Information Technology Act, 2000

[101] Ibid 99 Pg. 28

[102] Section 75, Information Technology Act 2000

In the year 2011, the Indian government installed a Centralized Monitoring System (CMS). This was done under section 5(2) and rule 419A under the Indian Telegraph Rules, 1951.[103] This system allows the government to tap telephones and intercept communications in a situation of 'public emergency'. Therefore, the government can order to intercept if there is a concern regarding interests of the sovereignty and integrity of India, security, friendly relations with foreign states, public order and for preventing incitement to the commitment of an offence.[104] Human Rights watch claims in an article that[105] the new monitoring system in India threatens the fundamental rights. The report suggests that the Indian government did not release information about the surveillance, for example who may authorize it, what are the legal perquisites that must be met while intercepting. It further stipulates that a lack of data protection legal framework gives the government more leverage to act arbitrarily and misuse its powers. There have been instances where surveillance was used by government officials and bureaucrats for political reasons instead of security purposes. Moreover, Indian activist have time and again revolted against the concerns of CMS and have stated that it hinders their right to privacy and freedom of speech and expression. Report also suggests that India has a bad history with violating its citizens fundamental rights. The government has put pressure on Google and Facebook to block content, impose liabilities and have furthermore, arrested people for posting content that is critical about the government.[106]

The freedoms and fundamental rights of the citizens were once again questioned when India adopted the 'Digital India' program. This program aimed to empower the country and promote e governance.[107] As part of this program Aadhar Card was introduced, which is a national identification card having a unique number for every citizen (similar to Norwegian *personnummer*). Later, the Aadhar Act 2016 was adopted to further institutionalize promote the Aadhar system. Every citizen was to apply for a Aadhar card and in or der to obtain this, citizens were to provide with large amount of personal data, including biometric and geo location data. All the personal data is stored in a centralized database that is under a central government authority, called Unique Identification Authority India (UIDAI).[108] The Aadhar

[103] This section and the rule under provides procedures for the government to tap telephones.

[104] Section 5(2) & Rule 419A, the Indian Telegraph Rules 1951

[105] Available https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights

[106] Available https://www.aljazeera.com/news/2022/2/5/india-muslim-activist-jailed-for-a-speech-completes-two-years-in and https://freespeechcollective.in/2022/07/01/with-13-mediapersons-in-custody-in-india-whither-free-speech/

[107] Available https://www.digitalindia.gov.in/

[108] Ibid 99 Pg. 29-30

Card is used for opening a bank account, filing in tax returns, applying for social security benefits etc. Under Section 33 (2) of the Aadhar Act, it allows the disclosure of all personal information, including identity and authentication information in the name of national security and integrity. Moreover, section 57 of the Act allows private parties to use the information to authenticate identity of a person. Although the judgment provided by Justice Sikri states that 'the owner of the information shall be given the opportunity to be heard before issuing such orders under section 33.[109]' The provisions under this Act also apply to foreigners who have resided in India for a period of one hundred and eighty-two days or more in the twelve months immediately preceding the date of application of enrollment.[110] Therefore, meaning that the Indian government will have access to foreigners' data as well, as it will be in the database.

Chapter 4 Privacy Paradox

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

K.S. Puttuswamy vs Union of India (2017)

Previously in part III, we discussed India's current data privacy regime. It was concluded that the current legal framework does not provide a sufficient or equivalent safeguard regarding data privacy. Therefore, India is currently transitioning from an old framework to a new one. Some scholars argue that India is trying to replicate the GDPR[111], but in fact, only a comparison can yield insight. India has various reasons to enact such a Bill, personal reasons such as protection of legislation on which the government programs such as Digitalize India etc. depend and protect privacy. On the other hand, another reason behind the Bill is to obtain a positive adequacy assessment from the European Union under Article 45 GDPR.[112]

The GDPR came into effect in May 2018 and ever since then many countries have tried to implement data protection laws or are in the process of implementing them and India is one of

[109] Available https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

[110] Section 2 (v) Aadhar Act, 2016 Available https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

[111] Committee of Experts under the Chairmanship of Justice B N Srikrishna, *"Draft Personal Data Protection Bill, 2018*," July 27, 2018, https://www.thehinducentre.com/resources/ article24561526.ece/binary/Personal_Data_Protection_ Bill,2018_0

[112] G. Greenleaf, UNSW Australia 163 Privacy Laws & Business International Report 1 2020, 6-9

them.[113] The Modi government submitted the PDPB to the Lok Sabha, the lower house of the Parliament. The PDPB is based on the Bill that Justice BN Srikrishna Committee drafted. In July 2017, this committee including many experts was appointed by the Indian government on Data Protection Framework for India. The committee, under the chairmanship of Justice B.N. Srikrishna drafted the PDPB. They suggested that India needed a strong Bill, and it was in the interests of the citizens, businesses, and the Indian government.[114] The committee attempted to adopt a GDPR-style data protection regime in India. However, it failed to weigh the economic costs and benefits of implementing it[115] Burman argues that in an emerging economy like India, evaluating the direct and indirect costs of such legislation is essential. I agree with the author that further research on data protection laws is required in India. Nonetheless, the bill was proposed in the Indian Parliament called the Personal Data Protection Bill.

It would therefore be interesting to critically analyze the Bill and its main elements and compare it with the GDPR. The idea of comparison is to help businesses understand the deviations from the GDPR. Before we dive into the topic, it would be important to note the significant roles in the PDPB. Similar to the GDPR, the PDPB refers to the data processors as data processors[116], but data controllers are called data fiduciaries[117] and data subjects as data principals[118].

1. **Scope**: Not only do both the legislations apply to citizens of their respective jurisdiction, but also to organizations and companies that are established outside the jurisdiction. For example, the PDPB states "Organizations that are not present in India but process personal data in connection with (i) business carried out in India or any systematic offering of goods or services to individuals in India, or (ii) an activity that involves profiling individuals in India.[119] A very good analysis of the comparison is provided by Covington & Burling, that states that the PDPB has a broader scope than the GDPR as an entity might

[113] A. Burman *Will a GDPR Style Data Protection Law work for India,* 2019 Available https://carnegieendowment.org/files/4-17-19_Burman_India_GDPR.pdf Page 1

[114] Ibid 111

[115] Ibid 113

[116] Section 3 PDPB, an individual who is not an employee of the fiduciary and processes data on behalf of the fiduciary is the data processor.

[117] Section 3 PDPB, an individual who alone or in conjunction with others, ascertains the objective and mode of processing of personal data is the data fiduciary.

[118] Section 3 PDPB The natural person who is the subject of personal data is known as the natural person.

[119] Section 2 A(b) Protection of Personal Data Bill, 2019

fall under the scope of PDPB if personal data is processed through the use of a processor. This can only be exempted if the Government of India exercises its authority and decides to exempt such processing activity.[120] Considering the subject matter scope, the GDPR applies to personal data and keeps the anonymous data out of scope. On the contrary, the PDPB authorizes the government to seek access to anonymous data, personal data or non-personal data when required. The government may hold authority to do so when it comes to prevention or detection of a criminal offence.

2. **Definition of Personal Data:** Under the PDPB the term personal data is defined as 'means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information'[121] One of the major differences is that the personal data under the GDPR relates to an identifiable person, whereas the PDPB takes a broad perspective here and discards the likelihood of an individual getting identified.
3. **Sensitive Personal Data:** In addition to all the special category data that GDPR offers, the PDPB also classifies financial data, caste, or tribe data as sensitive data. Under the GDPR, the list is well defined, whereas the PDPB allows the government to add additional data objects. One of the main differences as laid down by Covington is that the GDPR offers additional rules for processing criminal rules for processing data relating to criminal conviction and offences. Whereas the PDPB does not require such a provision.
4. **Core Principles:** The core principles of the GDPR are laid down in Article 5, such as lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; integration and confidentiality and accountability.[122] The PDPB directly doesn't refer to principles but lays down similar provisions yet has the following provisions:
   a. Section 4 lays down that Personal data to be processed for clear, specific and lawful manner.
   b. Section 5 states the principles of fairness and reasonableness, purposefulness and promotes data privacy of the data subject.

---

[120] Covington & Burling *Comparison- Indian PDPB Bill 2019 vs GDPR* 2020 Available https://www.privacysecurityacademy.com/wp-content/uploads/2020/05/Comparison-Chart-GDPR-vs.-India-PDPB-2019-Jan.-16-2020.pdf

[121] Personal Data Protection Bill 2019 Pg. 5 Available https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[122] Article 5 General Data Protection Regulation, EU 2016/679 2018

c. Section 6 states that the processing of personal data shall only be carried out to the extent it is necessary.

d. Section 8 puts responsibilities on the Data fiduciaries must take necessary steps to implement the data protection principles. For example, data to be processed," considering whether (a) the data is likely to be used to make a decision about the data principal, (b) the data is likely to be disclosed, or (c) is kept in a form that distinguishes facts from opinions or personal assessments. In addition, the data fiduciaries are not allowed to retain personal data for more time than it is necessary. The retention can only happen if there is an explicit consent from the data principle or is specified in regulations.

e. Lastly, it is the duty of the Data fiduciaries to comply with the provisions of the act.

It can therefore be concluded that the PBPD does replicate the GDPR when it comes to the core principles, but it can be critiqued that no principles of confidentiality, integrity are specified in the Bill. On example, where the PDPB takes a different approach is that it requires deletion of all data whereas the GDPR permits that personal data can be retained after the purpose is over only if it is anonymized.

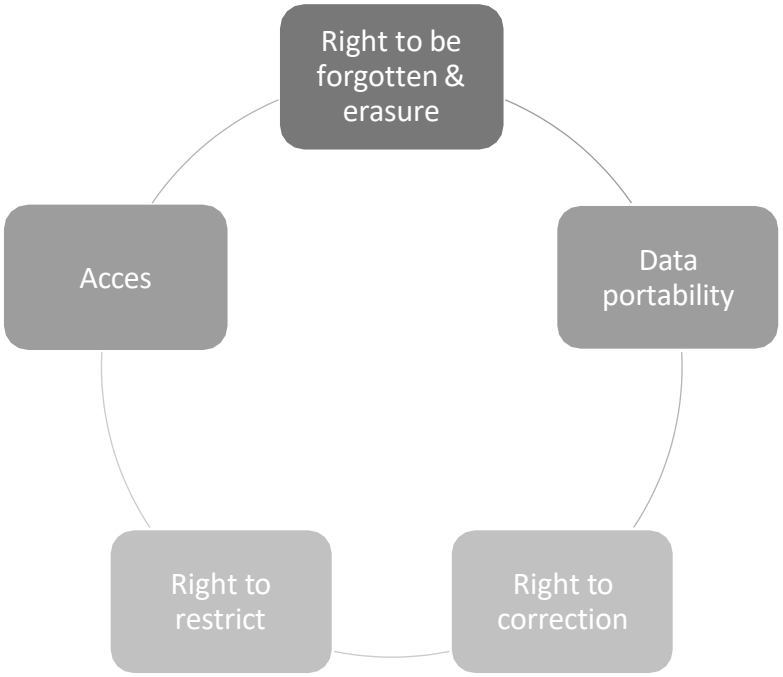
5. **Legal basis for processing the data & legitimate interest**: there is where one sees some deviation from the GDPR. For example, the PDPB does not consider performance of a contract one of the legal basis for processing data. One could argue that consent covers both the aspects of explicit consent and through a contract signed by the data principle. Yet I argue that it would be hard to establish that, especially when consent can be taken back. There are additional grounds for 'reasonable purpose' in section 17 for example,

(a) the interest of the data fiduciary in processing for that purpose; (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal; (c) any public interest in processing for that purpose; (d) the effect of the processing activity on the rights of the data principal; and (e) the reasonable expectations of the data principal having regard to the context of the processing.[123] It shall be noted that the PDPB allows the Data Protection Authority to lay down reasonable grounds for legitimate interests rather than the data controller, as in GDPR. Under the GDPR, many companies rely on legitimate interests for processing of data, but the PDPB takes a strict approach here.

[123] Ibid 121

6. **Conditions for processing sensitive data**: Both the GDPR and the PDPB have similar grounds to process data based on consent, such as, consent shall be explicitly obtained[124]. Under the PDPB, the sensitive personal data shall not be processed for the purpose of employment, whereas the employer will have to reply on explicit consent of the employee. In order to keep a check on the consent, the PDPB also has an entity called a consent manager[125].

7. **Data subject rights**: The PDPB dispenses various rights to the data principles, for example, right to consent, the data principle can decide as to who can have access to their data, they have right to correction, data portability, right to be forgotten, erasure of data that might be irrelevant or outdated, right to restrict the continuity of data disclosures.[126]



8. Data localization requirements: This is a topic that doesn't find place in the GDPR other than if data transfer requirements are not met. On the contrary, the PDPB states that 'The Central Government shall notify categories of personal data as critical personal data

[124] Ibid 112 Article 7

[125] The PDPB lays down that a consent manager is an independent entity that shall manage data principles consent in a secure, transparent manner. Available here https://iapp.org/news/a/consent-manager-framework-under-indias-personal-data-protection-bill/#:~:text=What%20are%20consent%20managers%3F,interoperable%2C%20secure%20and%20transparent%20platform.

[126] Ibid 121

that shall only be processed in a server or data center located in India.' In addition, it is within the powers of the government to decide what can be termed as critical personal data.

9. **International Data Transfers:** The GDPR provides data transfer to outside of EU and EEA if one of the criteria is met under Chapter 5, such as adequacy decision, appropriate safeguards, binding corporate rules etc. Whereas, under the PDPB a copy of personal data can only be transferred outside India if:) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or (b) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organization is permissible; or (c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or (d) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or (e) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified under sub-section (2) of section 40(Restrictions on Cross Border Transfer of Personal Data)[127]

10. **Anonymized data:** The GDPR does not define anonymized data, but the regulation does not apply to anonymized data (Recital 26). Similarly, the PDPB does not include anonymous data as personal data, but the government is allowed to ask for access of anonymized data under the PBPD.

11. **Others:** In most of the other areas, the GDPR and the PBPB are a bit similar and have a few deviations such as penalties, information security, appointment of processors yet there are some areas where the deviations are broader. In terms of social media and data privacy, it is indeed interesting to know that under the PDPB the social media intermediaries are considered as data fiduciaries.

Conclusion: Although India is taking a step ahead in the data privacy sphere, be it to protect the fundamental rights of the individuals or to gain sovereignty over its data. India has attempted to adopt a framework that only time can tell whether it promises safeguards and measures. The Bill is in the parliament and is yet to be passed as an act in the second half of 2022. Nonetheless, it has received criticism and praises from various scholars. For instance,

[127] Ibid 121

the Internet Freedom Foundation writes that[128] the ownership of user data is vaguely defined. They cite an example of Brazils General Data Protection Law, which has explained that every natural person is assured ownership. The author argues that, under the PDPB it leaves room for ambiguity.

Another criticism that I agree with is that Section 91 provides that the government can have access to anonymized data or non-personal data. Do they have a provide an explanation for processing or collection of such data? No. Therefore, it nullifies the right to privacy when it comes to the authority the government holds.

Chapter 5 Future of India

In the previous part we saw the main differences between the GDPR and PBPD, it was academic research and therefore I decided to take a different approach for this part. Therefore, this part is divided into two parts. For the first part I got the chance to interview a data privacy rights activist in India. Apar Gupta, a lawyer, an activist and a technology, democracy and digital rights writer shared his thoughts about what the future of India looks like. For the second part I analyze the upcoming PDPB bill in light with the guidelines laid down by Lee Bygrave.

Question 1

Do you think there has been a positive impact on data privacy rights after the Puttaswamy judgment?

Answer: Before the Puttaswamy judgment, privacy was not a prominent feature of the Indian governmental system in terms of legislation and policymaking. For instance, in the National Economic Survey of 2018 and 2019[129], it was highlighted that privacy is an 'elite concern'. Policies that the Indian government commenced never had privacy as the central aspect. However, one notices that post the Puttaswamy judgment. There has been a display of 'privacy' in the policies. He asserts that these are indicative of incentives for the private sector. However, the private and public sector boasts the Puttaswamy judgment and has conspicuous and

[128] Available https://internetfreedom.in/privacyofthepeople-social-media-users/

[129] Available https://www.thehindu.com/news/national/centres-aadhaar-affidavit-in-supreme-court-welfare-of-masses-trumps-privacy-of-elite/article18951798.ece

substantive characteristics of fundamental rights, yet there is a high disconnect between such statements and enforcement.

Question 2

Do you think the PDPB strengthens the state or the citizens?

To this answer, Apar stated that the risk comes from the nature of the Indian society. As people are not aware of their rights, of the new act, therefore it leads of lack of autonomy on one's personal data. This is relevant in both private and public sector. For example, in the public sector the people do not yet have the right to correction, erasure etc. therefore leading to not getting access to social benefits such as pension, subsidiaries etc. It shall therefore be looked at the point of view of the data principles and not an act that will ease businesses.

Question 3

What areas you think the PDP bill should be modified, what can India do so that they do not fall in the same category as the US (Privacy Shield invalidated).

According to Apar, the existing PDPB does a poor job about being a data protection bill per se. For example, it talks about regulating social media intermediaries. Another example pointed out by Apar was that the PBPD requires people to link their government identification documents (voter ID, social security number etc.) with their social media account. This would not only provide government more access but also hamper the privacy of the data principles. Therefore, the bill requires deeper study and needs a strong legislation. One of the biggest dangers in India is very similar to that of the US. The absence of a data protection law has given leverage to many private sectors to exploit the system and therefore undermine the trust of users[130]. In the name of creating a digital society, user rights are undermined. People talk about digital dystopia rather than digital utopia. Therefore, more than focusing on transfers and what it means to the business, the PBPD shall focus more on privacy rights.

[130] Referring to the Facebook Case https://www.bbc.com/news/technology-54722362

Question 4

In your general opinion how the situation regarding rule of law, constitution and fundamental rights in India is. Do the policymakers take these aspects seriously or not? What is lacking in the Indian legislative system?

Apar emphasized that India has never indeed had a good rule of law system, indicating that there is no predictability in the given application of the law. The primary reason behind his argument was the nature of Indian society. India faces various challenges such as gender, caste, and economic status discrimination. These discriminatory elements are determining elements as to what the legal outcome will be. The interaction of these factors with the law also determines what kind of legal advice and representation a person will receive. Apar points out that this differs from how the rule of law is perceived in Europe. Talking of the Indian judicial system, he refers to the system as a monolith that displays vices on the line of language, caste, and gender.

Moreover, the Indian constitution pledges a social transformation that considers a holistic concept of fundamental rights that, in his words, is an aspiration and not altogether fulfilled. Finally, he pointed out that technology will only deepen the divide. In his opinion, the PDPB is simply an aspiration requiring in depth work. Although all the opinion is based on a proposal and not an act yet, therefore only time can tell how successful the Act will be.

For the second part of this question, we analyze the upcoming PBPD in the light of four elements that are argued by Lee Bygrave in his book. Lee states that '[131]data privacy law specifically regulates all or most stages in the processing of data'. He states that data privacy law aims to protect and safeguard the fundamental rights of the individuals (data principles/ subjects) light of principles laid down by lee Bygrave. Lee Bygrave argues that the framework of data protection shall entail the following[132]:

1. Single statute legislation to ensure clarity and coherence
2. Independent enforcement body to oversee the implementation of legislation
3. The broad framework of laws to enable smooth adoption of modifications in line with the changing needs of technology and innovation

---

[131] L.A. Bygrave *Data Privacy Law: International Perspective* 2014 Available https://doi.org/10.1093/acprof:oso/9780199675555.001.0001 Pg. 1

[132]Ibid 131

4. Advisory body for the regulator to aid effective understanding and implementation of laws by the enforcement body

1. When talking of single legislation to ensure clarity and coherence, Lee argues that data privacy should be largely statutory. He further states that it is also necessary to take into consideration case laws, soft law, such as guidelines, recommendations, and code of conduct [133]In terms of India there is yet no clarity as of now but once the Bill is passed and is enacted, there will be single a single statute on personal data protection. Secondly, there are various case laws that emphasize that right to privacy is indeed a fundamental right. Moreover, India is a signatory of many international treaties that respect fundamental rights such as the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, International Covenant on Economic, Social and Cultural rights.
2. Secondly, Lee argues that data privacy statues shall establish special independent bodies to oversee their implementation.[134] Here he refers to Data Protection Authority that looks over and regulates data processing activities. The PBPD in Section 49 reflects on an independent regulatory body, therefore indicating 'independence'. Yet, the Government can issue the authority directions which are not subject to judicial review (Section 98). Secondly, when it comes to the structure of the Data Protection Authority, it is important to note that the Bill under Section 68 states that there shall be a separate adjudication department within the Authority. This department shall have the responsibility to decide penalties and compensations. Currently, it is unclear as to how these adjudicating bodies will be appointed. It is also unclear as to how these authorities will work. A very interesting argument on this point is enunciated by the authors of Dvara Research paper[135] is that this authority will be looking after close to 60 million establishments (excluding public administrations, defense, and other state bodies). Almost all these establishments will be processing large amounts of data. This poses more risk to the individuals and therefore, a risk-based supervision using a responsive regulatory tool shall be used.
3. The third element laid down by Lee is that generally all the data privacy statues take an approach that is called 'framework' law. On this point I agree with the author as

[133]Ibid 131 Pg. 3

[134] Ibid 131 Pg. 3

[135] Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools Dvara Research, July 2018 Page 6

technology is fast moving and having a regular framework based on what exists now can pose various challenges. The PBPD does not deploy detailed rules on processing or is missing a practical element. If there are to be any amendments, it is essential that the amendments are passed by simple majority in both the houses.

4. Lastly, Lee argues that the Data Protection authorities shall play an important advisory role in the practical elements of data protection, for example the data protection authorities in Denmark, Norway, or the UK. In terms of the PBPD, the Data Protection Authority shall be doing the following under Section 60:

i. *promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data, including issuance of any public statement setting out trends in, or specific instances of, contravention of the 34 provisions of this Act by a data fiduciary or a class of data fiduciaries, as the case may be.*

ii. *promoting awareness among data fiduciaries of their obligations and duties under this Act.*

iii. *monitoring technological developments and commercial practices that may affect protection of personal data.*

iv. *promoting measures and undertaking research for innovation in the field of protection of personal data.*

v. *advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of this Act.*

vi. *issuing guidance on any provision under this Act either on its own or in response to any query received from a data fiduciary where the Authority considers it necessary, subject always to the provisions of this Act.*

vii. *advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data;*[136]

Therefore, it can be concluded that the Data Protection Authority will play a role of an advisory body. There might also be a downside to this, for example, Lee argues that there are various risks involved in this[137]. One such issue is that when it is indeed the duty of the Data Protection

[136] Available https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf Page 34

[137] Ibid 131 Pg. 4

Authority to promote data privacy and advice on new rules, new technological developments etc., it can be hard for the other organs of the government to keep up with that. Lee enunciates that *"[..]courts' frequent lack of familiarity with the legislation, combined with the time pressures of litigation, can result in their failing to appreciate the complexities of the legislation in ways that undermine the correctness of their judgments''*

CONCLUSION

This master thesis is an attempt to analyze the data protection regime in India. The thesis was introduced with the topic of data privacy and how states all over the world are regulating and trying to regulate the data privacy laws, either to attain sovereignty over data or to tighten the rules to protect the fundamental rights of the citizens. In chapter I, outsourcing, I analyzed why India is an ideal destination for outsourcing and therefore, it was concluded that there are various political and legal reasons for India being a leading country in outsourcing. In chapter II we were able to answer the question of whether privacy is dead and concluded that states are initiating legislation that protects privacy and data privacy. Chapters III, IV and V focus on India, and we see that although the laws and the case laws state that India is a democratic state that has signed and ratified various international treaties, there have been examples of various infringements. Furthermore, I analyzed the Indian laws in the light of the four essential guarantees but concluded that in the existing legislation, one witness's deviations and, therefore, India does not provide equivalent protection. Although. After having analyzed the upcoming Bill (withdrawn on August 3, 2022), it can be stated that it does not fulfill the criteria and requirements as that of almost equivalent protection. Yet on the other side, it does try to embed the values of the GDPR. For example, the establishment of an oversight mechanism and much clearer and more precise rules to have access to data. Nonetheless, how well the new Bill is adopted and how well the legislators take from the PDPB Bill is a question that only time can answer. It was initially stated that the Bill would be passed in the second half of 2022, but as per the latest development, it is stated that the Bill has been withdrawn. Moreover, it was further stated that a new Bill, which will be built based on the Protection of Personal Data Bill, 2019 and will adopt more international measures. Therefore, it can be concluded that the withdrawal of the Bill states the unsatisfactory end of a long and tedious process. The upcoming Bill will be initiated in the month of February 2023.

Therefore, only time can tell whether India can have GDPR-style legislation or will take its own approach and will be a balance between the interests of the state and the fundamental rights of the citizens. I am hopeful that the Bill will be more up-to-date, especially after the recommendations of scholars and experts from various occupations. I am also hopeful that the government takes into account all deliberations and has an independent and diverse group of experts. In chapter V, I concluded that despite India having rule of law, fundamental rights yet there have been instances of breaches in various fields. Therefore, there is an urgency to protect data privacy in India, and this was also emphasized by the Puttaswamy judgement and the Sri Krishna committee. Although there is no proper legal regime that protects data and its privacy, yet there is hope Judgments like Puttaswamy give hope to a new and modern India that gives utmost significance to fundamental rights and privacy rights of individuals. I conclude by agreeing with the internet freedom foundation 'each day lost causes more injury and harm. As we await an open, trustworthy, and accountable public consultation process held in good faith on this new framework.'[138]

[138] Available https://internetfreedom.in/here-lies-the-data-protection-bill-2021/

REFRENCE LIST

Books

John S. Mill, *'On Liberty'*, Batoche Books 1859

P Voight & A. von dem Bussche the EU General Data Protection Regulation (GDPR) A practical Guide 1st edition, Springer 2017
L. Bygrave (2014). *Data privacy law: an international perspective.* Oxford, Oxford University Press.
B. Vagadia *Outsourcing to India Legal Handbook* 2nd edition

International Regulation

Universal Declaration of Human Rights
International Covenant on Civil and Political Rights

International Covenant on Economic Social and Cultural Rights

California Consumer Privacy Act

European Regulation

The General Data Protection Regulation, 2016/679

European Convention on Human Rights

Indian Regulation

Code of Criminal Procedure 1874

Personal Data Protection Bill 2019

Information Technology Act

SDPI Rules or the Information Technology (Reasonable security practices and procedures and sensitive personal data or information)

The Indian Telegraph Act 1885

The Information Technology (Procedure and Safeguards for interception and decryption of information) Rules, 2009

Constitution

The Companies Act, 2013

The Competition Act, 2002

Aadhar Act 2016

Case laws

Judgment of the Court (Grand Chamber) of 16 July 2020. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Request for a preliminary ruling from the High Court (Ireland).

Justice KS Puttaswamy and Anr Vs. Union of India 2017 10 SCC

State of Punjab vs Gurmit Singh 1996

Karmanya Singh Sareen v Union of India WP(C) 7663/2016

Bachan Singh vs State of Punjab 1980

MP Sharma Vs Union of India (1954)
Kharak Singh Vs. Union of India (1964)
Wolf V Colorado 1949 238 US 25
Peoples Union of Civil Liberties Vs Union of India 2001

Articles & Journals

E. Kiesow Cortez, *Data Protection Around the World, Information Technology and Law Series 33*, 2021
M. Zalnieriute, *Data Transfers after Schrems II The EU UD Disagreements over Data Privacy and National Security* 2022
B. Patricia. *Book Review*: *Data privacy law: an international perspective, by Lee Bygrave, Oxford, UK, Oxford University Press, 2014, XXIX, ISBN 978-0-19-967555-5. Information & Communications Technology Law.* 2015

A Gonzales & Others *Outsourcing: Present, Past and Future* 2004

S. Hilley, *when you outsource to India, where does your data go: Not where you think* Computer Fraud & Security. Issue 6, 2004
M Ziegele, O Quiring *Privacy in Social Network Sites 2011*
Y. Poullet, *Data Protection legislation: What is at stake for our society and democracy?* Computer Law & Security Review 25, 2009
M. C. James, "*A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe",* Connecticut Journal of International Law Vol. 29, Issue 2, 2014
Warren and Brandeis, "*The Right to Privacy", Harvard Law Review*, Vol.4, No. 5 1890
F. DeBrabander. *Life after Privacy: Reclaiming Democracy in a Surveillance Society*. Cambridge: Cambridge University Press 2020
V. Boehme Nebler *Privacy: a matter of democracy. Why democracy needs privacy and data protection* International Data Privacy Law Volume 3 No. 3 2016
The Joint Parliamentary Committee, India in its recommendations refers to the GDPR in various areas.
Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. IndraStra Global
Srivastava, A. (2019). Data protection law in India: the search for goldilocks effect. European Data Protection Law Review (EDPL), 5(3), 408-415.
Ashit Kumar Srivastava, Data Protection Law in India: The Search for Goldilocks Effect, 5 EUR. DATA PROT. L. REV. 408 (2019).
Monika Zalnieriute Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security January 2022
C. Ramachandran PUCL v Union of India Revisited: Why India's Surveillance law must be redesigned for the digital age.
Chowdhury, P., Thayil, K., 25 January 2021, Data Privacy in India
Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Draft Personal Data Protection Bill, 2018," July 27, 2018, https://www.thehinducentre.com/resources/ article24561526.ece/binary/Personal_Data_Protection_ Bill,2018_0
Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia (2020) 163 Privacy Laws & Business International Report 1, 6-9
Will a GDPR Style Data Protection Law work for India, Anirudh Burman available https://carnegieendowment.org/files/4-17-19_Burman_India_GDPR.pdf
Covington & Burling Comparison- Indian PDPB Bill 2019 vs GDPR
Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools Dvara Research, July 2018

Reports & Recommendations

European Data Protection Board *Government access to data in third countries*, November 2021. Available legalstudy_on_government_access_0.pdf (europa.eu)

Other Projects & Initiatives | Ministry of Electronics and Information Technology, Government of India (meity.gov.in)

Shara Monteleone, Members Research Service European Parliamentary Research Service
NASSCOM Implications of Schrems II on EU India Data Transfers August 2021. Available https://nasscom.in/sites/default/files/202108_NASSCOM_Schrems_II_Study.pdf

Indian Law Websites

IndianKanoon.org

Scconline.in

Electronic Sources

https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682

Govt withdraws Data Protection Bill, 2021, will present new legislation | Business Standard News (business-standard.com)
https://stpi.in/en/about-stpi#:~:text=The%20first%20historic%20event%20that,Software%20Technology%20Parks%20of%20India.

https://www.opindia.com/2019/03/digital-india-how-the-modi-govt-took-massive-strides-in-turning-india-into-a-digitally-empowered-economy/

https://www.statista.com/statistics/1102329/india-number-of-colleges/

https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/about-us/analystreport/TCS-Leaders-Ovum-Decision-Matrix-Selecting-Core-Banking-System-in-European-Market-2016%E2%80%9317.pdf

https://www.umsl.edu/~siegelj/information_theory/projects/Bajramovic/www.umsl.edu/_abdcf/Cs4890/link1.html

https://www.ciodive.com/news/data-privacy-CCPA-GDPR-fines/572077/
https://www.dataguidance.com/resource/definitive-guide-schrems-ii#supplementary%20measures
https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html
https://lawsisto.com/legalnewsread/ODk4Mg==/Judgement-Analysis-K-S-Puttaswamy-and-Ors-v-Union-of-India-2017-10-SCC-1
https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf
https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
https://indiankanoon.org/doc/911085/

https://indiankanoon.org/doc/1439440/
https://www.jagranjosh.com/general-knowledge/article-32-of-indian-constitution-1605699265-1
https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/india/ https://www.india.gov.in/my-government/constitution-india#:~:text=The%20Republic%20is%20governed%20in,force%20on%2026th%20January%2C%201950.
https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights
https://www.aljazeera.com/news/2022/2/5/india-muslim-activist-jailed-for-a-speech-completes-two-years-in
https://freespeechcollective.in/2022/07/01/with-13-mediapersons-in-custody-in-india-whither-free-speech/
https://www.digitalindia.gov.in/
https://iapp.org/news/a/consent-manager-framework-under-indias-personal-data-protection-bill/#:~:text=What%20are%20consent%20managers%3F,interoperable%2C%20secure%20and%20transparent%20platform
https://www.thehindu.com/news/national/centres-aadhaar-affidavit-in-supreme-court-welfare-of-masses-trumps-privacy-of-elite/article18951798.ece

https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf