LEGAL PROTECTION OF RIGHT TO PRIVACY IN CYBERSPACE

DISSERTATION

SUBMITTED TO:

National Law School of India University, Bengaluru

UNDER THE SUPERVISION OF:

Prof. (Dr.) A. Nagarathna
National Law School of India University,
Bengaluru

SUBMITTED BY:

Namrata Behera
LLM/941/2020

CERTIFICATE

This is to certify that this dissertation titled 'LEGAL PROTECTION OF RIGHT TO PRIVACY IN CYBERSPACE', submitted by Ms. Namrata (ID No. 941) in partial fulfilment of the requirements of LL.M. Degree for the academic session 2020-21 at National Law School of India University, Bengaluru, is the result of bonafide research carried on by her under my guidance and supervision.

PROF. (DR.) A. NAGARATHNA
NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BENGALURU

Date:

Place:

DECLARATION

I, the undersigned, solemnly declare that this dissertation titled as 'LEGAL PROTECTION OF RIGHT TO PRIVACY IN CYBERSPACE', submitted to National Law School of India University, Bengaluru for LL.M. Degree (2020-21), is an original and bonafide research work carried out by me under the supervision of my guide. All sources used in this dissertation have been duly acknowledged and credited. The information contained in this work is true to the best of my knowledge. This dissertation has not been submitted for any degree, fellowship or diploma.

Namrata Behera

LLM/941/2020

LLM (Business Laws)

ACKNOWLEDGMENT

I would like to take this opportunity to express my deepest gratitude to everyone who helped me to complete my dissertation.

I would like to express my heartfelt gratitude to my supervisor, Prof. Dr. A. Nagarathna, for her invaluable guidance and support. The task would not have been completed without her direction and encouragement. Because of her patience, drive, passion, and vast knowledge, I was able to finish my dissertation.

I would like want to thank the NLSIU library for the abundance of data and the library team for their continued support.

I would also like to thank my family and friends for always motivating and supporting me which helped me to complete my dissertation work.

LIST OF ABBREVIATIONS

IT	Information Technology
EU	European Union
PDP	Personal Data Protection Bill
GDPR	General Data protection Regulation
ICT	Information Communication Technology
US	United States
Covid -19	Corona Virus Disease, 2019
DPA	Data Protection Authority

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATUTES

1. The Constitution of India
2. The Information Technology Act, 2000
3. The Indian Penal Code, 1860
4. The Indian Telegraph Act, 1885
5. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
6. The Protection of Children from Sexual Offences Act, 2012

RULES

1. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
3. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

CASES

1. Maneka Gandhi vs Union of India, (1978) 1 SCC 248
2. MP Sharma vs Satish Chandra, AIR 1954 SC 300
3. Kharak Singh vs State of UP, AIR 1963 SC 1295
4. Govind vs State of Madhya Pradesh &Anr., (1975) 2 S.C.C. 148
5. R Rajagopal v State of Tamil Nadu, (1994) 6 S.C.C. 632
6. X vs Hospital, (1998) 8 S.C.C. 296
7. PUCL vs Union of India, (1997) 1 S.C.C. 301
8. District Registrar and Collector vs Canara Bank,(2005) 1 S.C.C. 496
9. Hindustan Times v High Court of Allahabad, (2011) 13 S.C.C. 155
10. National Legal Services Authority vs Union of India, (2014) 5 S.C.C. 438
11. Justice K.S Puttaswamy (Retd.) &Anr vs Union of India & Others,(2017)10 S.C.C. 1
12. Praveen Arimbrathodiyil vs. Union of India, W.P.(Civil) 18084 of 2021

CHAPTER I

1. INTRODUCTION

The technology that we utilise in our everyday lives is evolving rapidly. The way we produce, acquire, process, and exchange information are all being transformed through development in information technology. Electronic transactions and records are becoming increasingly important covering every sphere of our lives ranging from business activities to health care facilities.[1] The internet's meteoric rise symbolises this shift to a networked world. Due to the Covid-19 pandemic, we all had to make significant lifestyle changes. We all got the opportunity to become acquainted with a more digitally driven lifestyle than we had previously been. Whatever activity we undertake today is mostly done online, including our education, shopping, meetings, social events etc. In fact, many government operations are now being conducted online especially e-finance which has gained popularity recently. All of this has made us realize the importance of data, which is considered as "oil" of the digital era.[2] The use of cyberspace has become mainstream due to rapid technical breakthroughs. As the internet has grown rapidly, so have the risks connected with it. Humans have benefited from the usage of these technologies in a multitude of ways, including quicker communication, better education etc. The consequential effect of this has resulted in an increase in the demand for data privacy protection. Governments all across the world have utilised surveillance techniques to eavesdrop on private citizens, journalists, and human rights campaigners, thereby grossly infringing on their privacy. Furthermore, there have been several instances which suggest that private business organisations who gather data about their customer's online activity, have been found compromising with their privacy. In many nations where the "Right to Privacy" is regarded seriously, privacy in cyberspace is not just a need, but also a legal liability. Because the majority of an individual's data is now located on the internet, protecting privacy in this virtual domain is the need of the hour.

---

[1]Ryder, Rodney D., & Ashwin Madhavan, *Regulating Indian Cyberspace - The Battle for Control in the New Media Version 2.0*., 5 CONVERGENCE 250, 250-256 (2009).

[2]Sam Jossen, *The world's most valuable resource is no longer oil, but data*, The Economist, May 6th, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

This study analyses with the help of landmark judgements the importance and different facets by way of which right to privacy can be interpreted in India. It is, nevertheless, more pertinent in present day context as most of our work is done online, which can sometimes lead to breach of confidential information. The study also examines different provisions of the IT Act of 2000, as well as the applicable rules under it which act as a shield for data protection and therefore safeguard individual informational privacy in cyberspace. The study's findings also throw light on many key components of Indian legislation that needs to be improved in order to avoid tampering with individual data.

1.1. Statement of Problem

As the number of individuals who use the internet is expanding, absence of comprehensive and efficient data protection legislation would not only encourage greater privacy breaches in cyberspace, but also make it more difficult for enforcement agencies to deal with these concerns under current laws. Because of the fast-changing nature of the domain, it is critical that legislation governing cyberspace be examined and modified on a regular basis. Our government has been working on vital draft legislations, which is encountering delays until it is officially adopted as law of the nation. Hence, delays in enacting legislation costs citizens breach of their fundamental right to privacy while giving big tech companies more opportunity to maximize revenues without any fear of legal repercussions.

1.2. Importance of the study

With the progress of technology, a host of new problems have emerged. One of the most important consequences of technology is its influence on individual human rights, mainly in terms of privacy. Governments and profit-driven businesses have severely harmed the reasonable expectation of privacy. With the increased use of the internet and technology, particularly since the start of Covid-19, major issues revolving around data protection have arisen. To utilise the internet, one does not need to be an expert at it, and once any information is posted, it remains available to everyone across the globe. People consent to information access even when they are unaware of the repercussions. The Internet and Artificial Intelligence intrude on a person's personal space in unprecedented ways in human history. There is no doubt that the internet has made our globe more connected, but without strict adequate

regulations, this will have a negative impact on the society. More than ever, today is the perfect time when the right to privacy protection in cyberspace issue must be discussed and debated.

1.3. Aims and Objectives of the study

The goal of this thesis is to critically review and assess the available literature in order to identify gaps in the problems surrounding privacy issues in cyberspace. It further examines the origin of this doctrine under Indian constitutional jurisprudence while illustrating the numerous dimensions of privacy and how they correlate to the interpretation of legal requirements.

Objectives

1. To identify how the courts have defined the meaning and idea of the term Right to Privacy
2. To determine the impact of technological advancements on the right to privacy.
3. To analyse the relevant provisions of the IT Act, 2000 and the relevant IT Rules in terms of privacy protection in cyberspace.
4. To identify the inherent flaws and gaps within the legislative design and the regulatory framework and suggest reforms to address them.

1.4. Hypothesis

The privacy doctrine interacts with several other freedoms and values under the Constitution and the test of proportionality puts a check upon the arbitrary interference by the government authorities. Even though the IT Act, 2000 and IT Rules have been amended from time to time to meet the challenges of the present day, there is a huge information and awareness void in this area which requires active participation from all the stakeholders. In our increasingly networked and digital society, the information asymmetry between the individual consumer and the data collector, which is widening. Finally, our legal system is well-equipped to handle the technical and complex aspects of interpreting legal concerns in this subject.

1.5. Research Question

On the basis of the hypothesis taken, the researcher addresses the following research questions:

1. Whether right to privacy as a fundamental right is applicable to cyberspace?
2. Whether the traceability requirement under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 violated user's privacy and is against the Puttaswamy judgment?
3. Whether India should follow the European Union's data protection model or develop its own system which is comprehensive and ensures cost-effective protection for personal data?
4. What could be a practical strategy that could be adopted to resolving the problems related India's data privacy regime?

1.6. Research Methodology

The study is confined to a doctrinal approach and includes both primary and secondary sources. The information used is collected from legal and non-legal sources which includes cases, books, law reports, articles, blogs, reputed newspapers etc.

1.7. Mode of Citation

The citation is uniform throughout the dissertation and Harvard Bluebook citation method (19thedition) has been adhered to.

1.8. Scope and Limitation of Study

The dissertation employs a combination of analytical and descriptive methodologies, and it is limited to the Indian context, focusing solely on Indian legislation and the gaps that exist within it. This study is an examination of the researcher's observations, including references to prominent judgements, case reports, books, papers, and journals.

1.9. Review of Literature

- M.P. Jain, Outlines of Indian Legal and Constitutional History (Lexis Nexis 2014)

The author has focused on the advancement of the right to privacy as a constitutionally safeguarded right under Art. 21 of the Indian Constitution. The author has outlined the privacy jurisprudence and how it evolved through time via case laws and critical study of national and international legislations.

- Ashish Chibbar, Navigating the Indian Cyberspace Maze: Guide for Policy makers, (2020 ed., KW Publishers)

In this book, the author has given brief introduction to cyberspace. The book also discusses digital privacy concerns, issues related to cyber governance, cyber laws in India and lists down initiatives taken by the Government.

- NS Nappinai, Technology Laws Decoded, 1st ed, (Lexis Nexis 2017)

The book analyzes the relationship between the Constitution, Crimes, Intellectual Property Rights, and Contracts with technology laws, resulting in a new topic of study. Through extensive examinations of Electronic Evidence and Cyberspace Jurisdiction, the book addresses procedural complications. It also covers cyber terrorism, existing frameworks for cyber warfare, and cyber regulations for emerging technologies such as Cloud Computing, Drones, and the Internet of Things.

- Apar Gupta, Commentary on Information Technology Act - Along with Rules, Regulations, Orders, Guidelines, Reports and Policy Documents (Lexis Nexis 2016)

Information Technology Act of 2000 was passed with the intent of boosting the growth of electronic commerce, providing a legal framework, and preventing computer-related crimes in India. The commentary scrupulously covers all legislative and judicial changes in order to address current concerns and the evolving nature of cybercrime.

- Ryder, Rodney D., & Ashwin Madhavan, *Regulating Indian Cyberspace - The Battle for Control in the New Media Version 2.0*., 5 CONVERGENCE 250, 250-256 (2009).

In this article, the author discusses about issues revolving around informational security and data privacy. It also discusses various provisions under IT Act which deals with data protection regime in India.

- Atin Kumar Das, *Interface between Technology and Society: A Study of the Legal Issues*, 8 INDIAN JOURNAL OF LAW AND JUSTICE 120-127 (2017).

The author has explained the interaction between technology and society in this article. The article mentions about jurisdictional issues in cyberspace and main solution of this problem is that the enforcement measure should be global and secondly, in order to regulate cyberspace, governments must work together and coordinate their efforts.

- Umang Joshi, *Online Privacy and Data Protection in India: A Legal Perspective*, 7 NUALS LAW JOURNAL 95-111, (2013).

This article examines examine India's legal framework for internet privacy and data protection. It does not go into detail about the origins and evolution of the right to privacy, instead focus on the legislations that governs online privacy.

- Cassim, F. Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves. 18 POTCHEFSTROOM ELECTRONIC LAW JOURNAL 68-110 (2015).

The impact of identity theft crimes on people's personal information is examined in this article. It indicates that, in some nations, the rise in identity theft offences has resulted in the enactment of specialised legislation to combat the crime. The article investigates legislative remedies used to counteract or remedy similar crimes in South Africa, the United States, the United Kingdom, and India.

- Kritika Bhardwaj, Preserving Consent within Data Protection in the Age of Big Da*ta*, 5 NATIONAL LAW UNIVERSITY DELHI STUDENT LAW JOURNAL 100-110 (2018).

This paper examines the constitutional basis of consent and argues that it should be included in the data protection framework. It also discusses practical difficulties in implementing the consent principle and hence recommends for regulatory measures to enhance and strengthen the principle.

- Sougata Talukdar, Privacy and Its Protection in Informative Technological Compass in India, 12 NUJS L REV 287 (2019).

The idea of privacy is discussed in this article, as well as its acknowledgment in the Indian Constitution and the protection of informational privacy in the Information Technology Act of 2000.

- Vrinda Bhandari & Renuka Sane, Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018, 14 Socio-Legal Review 143.

Following the Puttaswamy decision, this article attempts to conceptualise the right to privacy and its consequences for both public and private actors. It contends that given the privacy concerns that have been raised in opposition to state action, the implementation problem in the domain of personal data will only become more difficult.

- Varun Kalra, and Ramisha Jain, An Armistice between Right to Privacy and Right of Surveillance, 4 INDIAN JOURNAL OF LAW & PUBLIC POLICY 1-23 (2017).

This paper aims to discuss the problems surrounding the right to privacy, comprehend the necessity for a complete privacy policy, and evaluate the use and abuse of surveillance rights.

1.10. Chapter Scheme

Chapter II: Cyberspace, Technology and Privacy: In this chapter, the researcher investigates the jurisprudential study of the evolving connection between technology and society and how it affects individual data privacy.

Chapter III: Interpreting the Concept of Privacy in India - As viewed by the Judiciary: In this chapter the researcher through an analysis of select cases examines the importance and different facets in which right to privacy has been interpreted in India. With time, Courts in India have broadened the horizons of privacy which duly covers in cyberspace as well.

Chapter IV: Comprehending relevant provisions of the IT Act and IT Rules: This chapter examines some of the provisions of the IT Act and the relevant IT Rules that protect individual data, while emphasising the critical necessity for a strong data protection law.

Chapter IV: Analysing Personal Data Protection Bill, 2019 And EU's General Data Protection Regulation: This chapter analyses key provisions of the PDP Bill 2019. It also examines whether India will benefit from EU-style data protection and finally what would be a more practical approach that could be adopted in resolving the problems related India's data privacy regime.

Chapter VI: Conclusion and Suggestions: The researcher closes the study with her thoughts on the overall functioning data protection framework in India and makes a few recommendations for improving the current regime in India.

CHAPTER II

2. CYBERSPACE, TECHNOLOGY AND PRIVACY

In this digital era, we are experiencing frequent technological developments and breakthroughs all over the world. The internet has undoubtedly brought about significant changes in the way society communicates, the services provided by the government, and the manner in which organizations engage. There is a growing interface between technology and society wherein, on one hand, advanced technologies assist to solve and alleviate a variety of issues in many sectors and on the other hand there is a continual concern that humans would become quiescent and excessively reliant on technology.[3] Before the digital age, information about an individual that may expose his or her identity appeared to be carefully managed, but this control is now eroding due to the rising interest in using the internet, which eventually leads to the exposure of personal data.[4] The entire globe is evolving into a digital environment in which the internet and information and communications technology play critical roles in the transmission of information.[5] Modern technical advancements in the field of computer science have evolved in such a manner that there is a comparatively inexpensive means for easy access to a vast and ever-expanding range of information on individuals residing worldwide. This may be determined by their age, gender, residential address, where and what they purchase, webpages they have visited and liked, and so on. As a consequence of their lack of knowledge and ignorance about how these sites function, an individual's privacy is violated.

All of this discussion portrays that there is a shift from the industrial to the technological era, which has resulted in the creation of a new domain called "Cyberspace". The word cyberspace does not have a single definition and is understood differently by different persons, nations, institutions, and authorities.[6] Cyberspace can be described as "*an artificial environment made up of interrelated*

[3]Atin Kumar Das, *Interface between Technology and Society: A Study of the Legal Issues*,8 INDIAN JOURNAL OF LAW AND JUSTICE 120-127 (2017).
[4]Id. At 3.
[5]Umang Joshi, *Online Privacy and Data Protection in India: A Legal Perspective*,7 NUALS LAW JOURNAL 95-111, (2013).
[6]ASHISH CHIBBAR, NAVIGATING THE INDIAN CYBERSPACE MAZE: GUIDE FOR POLICYMAKERS,(2020 ed., KW Publishers)

and intertwined networks that make use of electronic and electromagnetic spectrum-based ICT to generate, store, alter, share, and utilize information".[7] In simple words, a non-physical realm of information flow and communication between computer systems and networks is referred to as cyberspace.[8] The domain implies a "virtual space" although all information created is physically kept and can be copied and accessed. The cyberspace ecology runs on exchange of information. It is data which is of prime concern in cyberspace as there is a constant threat of information getting leaked or tampered with. In layman's terms, data is anything that represents information, knowledge, facts, concepts, or instructions.[9] Today, data is more than just information to be accessed in cyberspace; it is also a market worth millions of rupees.[10]With technological developments and their increasing utilization, there is a vast expanse of personal information transmitted across the internet. Social media, CCTV, drones, biometrics, are just a few examples of technologies that have a substantial impact on personal data security. Furthermore, while technological advancements provide several benefits, they do so at the expense of one person's enrich information potentially invading another person's privacy. The growing internet population has created new avenues for a myriad of issues, including cyber-attacks, which is one of the most pressing issues that the entire globe has been struggling to find a solution to.

Traditionally, individuals had greater privacy expectation from the State than from private actors. Governments have more influence in our lives, owing to their aggressive and policing powers, which include the ability to prosecute and punish, place citizens under surveillance, and even brutalise protesters. While surveillance has long existed, technical advancements have enabled the government to engage in unprecedented levels of electronic surveillance and predictive policing. With the rise of big data analytics, the expectations of the state and private players in terms of privacy concerns are blurring. Earlier only those at a higher socio-economic stratum enjoyed a greater degree of privacy than those at lower ones. Even today, different kinds of people have varied perspectives on privacy, and the majority of people are

---

[7]Id. At 6.

[8]Ian Carnaghan, *What exactly is cyberspace and cybersecurity?,* IN CYBERSECURITY (February 28th, 2011), https://www.carnaghan.com/what-exactly-is-cyberspace-and-cybersecurity/.

[9]Section 2 (o) of Information Technology Act, 2000.

[10] F Cassim, *Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves.* 18 POTCHEFSTROOM ELECTRONIC LAW JOURNAL 68-110 (2015).

still unaware of this right. Furthermore, they are also uninformed of the situations where their privacy rights can be compromised. In India, people have never placed as much emphasis on privacy as they do today. As a result, it is critical to comprehend the nature and scope of privacy. In today's society, privacy covers a wide range of rights and liberties. The freedom of expression, command over one's body and mind, information-based control, decision-making freedom, defence against surveillance/unwarranted invasion, protection against search and confiscation, right of personhood are all derived from the privacy principle.[11]

Privacy was foreseen long before the technical developments began, and it has been a notion that has been essential to humans since time immemorial.[12] The state of being free from public scrutiny, intrusion, or interference with one's activities or decisions is referred to as privacy. The right to exist in this state is known as the right to be let alone.[13] The right to privacy is a critical component of human dignity. Individual autonomy and everyone's right to make important decisions that impact the path of life are recognized by privacy. Privacy shields a person from the prying eye of the public in topics pertaining to his or her personal affairs. With time, courts in India have broadened the horizons of privacy which duly covers in cyberspace as well.

In this technological age, the concept of privacy is undergoing significant transformation. It is now widely understood that everyone requires privacy, however how it is valued varies by culture and differs from one person to person. In the case of information technology, concern for privacy is growing by the day, as advancement in this field is always accompanied with misuse, even when it benefits human civilization. The extent to which privacy is or should be legally protected is at the heart of the debate. In the next chapter we will look at the importance and different facets in which right to privacy has been interpreted in India with the help of few landmark judgements.

[11]Sougata Talukdar, *Privacy and Its Protection in Informative Technological Compass in India*, 12 NUJS L REV 287(2019).
[12]Frackman, Andrew J., and Martin, Rebecca C., *Surfing the Wave of On-Line Privacy Litigation*. THE NEW YORK LAW JOURNAL(2000).
[13]Samuel D Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193 (1890).

CHAPTER III

3. INTERPRETING THE CONCEPT OF PRIVACY IN INDIA – AS VIEWED BY THE JUDICIARY

3.1. Origin of Privacy Doctrine in India

The notion of "right to privacy" in simple words would mean right of an individual to be let alone.[14] It derives from the idea that certain rights and privileges are natural and intrinsic simply because of the fact that we are born as humans. As a result, certain rights are unassailable. In today's world, it is highly important and complicated, since information technology influences nearly every part of our life. Technology as we know it now is far distinct from what and how it was when our Constitution was penned. As a result, today's concerns must be resolved through a dynamic application of constitutional law and cannot be frozen in time. The constitution is always characterized as a living document for its potential to allow and apply principles in order to identify new solutions to the uncontrollable challenges we experience today.[15] The complex concept of privacy, as well as its importance in ensuring the proper application of the right to life under Article 21[16] of the Constitution, has strongly influenced India's 'privacy movement.'[17]Another important factor driving the expansion of privacy law is the ability to live with dignity.[18] Internationally, privacy is protected by a strong legal framework. Both Article 12 of the Universal Declaration of Human Rights, 1948 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966 guarantee legal protection against "arbitrary interference" with one's privacy, family, property, dignity, and reputation.[19] ICCPR was ratified by India on April 10, 1979 without reservation.[20]

---

[14]Id. At 13.
[15]B.K.Mishra, *Indian Constitution is a living document: Expert*, The Times of India, April 15, 2021,https://timesofindia.indiatimes.com/city/patna/indian-constitution-is-a-living-document-expert/articleshow/82071648.cms.
[16] INDIA CONST. art. 21.
[17] M.P. JAIN, OUTLINES OF INDIAN LEGAL AND CONSTITUTIONAL HISTORY (2014 ed. Lexis Nexis).
[18]Maneka Gandhi vs Union of India, (1978) 1 SCC 248 (India).
[19]Atin Kumar Das, *Supra* note 3.
[20]Krishnadas Rajagopal, *The lowdown on the right to privacy*, The Hindu, July 29, 2017, https://www.thehindu.com/news/national/the-lowdown-on-the-right-to-privacy/article19386366.ece.

Components of privacy also emerge in different situations from other aspects of freedom and dignity acknowledged and safeguarded by the fundamental rights included in Part III of the Constitution. Over the years, the Indian courts have sought to define the conceptions of privacy and the limits that can be inflicted. Before addressing privacy in the cyber age, let us first examine the evolution of the privacy doctrine in India broadly. The content of the constitutional right to privacy and its restrictions have been developed on a case-by-case basis, with every precedent attempting to build on and follow earlier conceptualizations which finally resulted in pronouncing right to privacy as a fundamental right.

One of the earliest cases that had only passing reference to the idea of privacy was *MP Sharma vs Satish Chandra*,[21] wherein the power of search and seizure by the State was held to be a reasonable restriction during the course of investigation. In this case, it was also argued that the right to privacy cannot be incorporated in the Indian constitution in the absence of a clause analogous to the Fourth Amendment to the US Constitution.In another interesting case, the *Kharak Singh vs State of UP*[22], the court recognized that domiciliary visits at night to be invalid. It recognized that the right to life guaranteed by Article 21 entails more than just animal existence. The Court decided that the right to privacy was not a guaranteed constitutional right, despite the fact that it acknowledged that domiciliary visits at night were illegal. In his dissenting opinion, Justice Subba Rao stated that the right to privacy is a fundamental component of personal liberty under Article 21 and hence, surveillance by State is unconstitutional.

Again, in *Govind vs. State of Madhya Pradesh*[23], an interesting observation was made as the Hon'ble Supreme Court accepted the right to privacy within a limited sphere and held not to be an absolute right. Reasonable restrictions can be imposed by the regulatory power of the State subject to compelling State interest. A decision that has assumed some significance is the case of *R Rajagopal v State of Tamil Nadu.*[24] In this case the right to privacy was raised to constitutional significance which stated that every citizen, including criminals, had the right to be left alone. The court further stated that public officials do not have a right to privacy with regard to their official

[21]MP Sharma vs Satish Chandra, AIR 1954 SC 300 (India).
[22]Kharak Singh vs State of UP, AIR 1963 SC 1295 (India).
[23]Govind vs State of Madhya Pradesh &Anr., (1975) 2 S.C.C. 148 (India).
[24]R Rajagopal v State of Tamil Nadu, (1994) 6 S.C.C. 632 (India).

actions and behaviour, because the general public has a right to know about their conduct. In addition, the court broadened the definition of privacy to include a person's, family, marriage, procreation, motherhood, childbirth, and educational privacy, among other things.

Sometimes revealing of factual information might have negative consequences for an individual, resulting in psychological issues. The Court dealt with similar kind of situation in the case of *Z*[25] wherein the court recognized right to privacy as an essential component of Article 21, although it can be restricted for the prevention of crime or the preservation of health or morality, or for the protection of rights and freedoms of others. The case of *PUCL vs Union of India*[26] portrays that Indian courts have time and again given due importance to the issue of privacy as in this case the court did not wait for the parliament to frame rules and therefore, it put forth certain procedural rules in the meantime. The court determined that phone tapping, unless done legitimately, would be a breach of Article 21 of the Indian Constitution.

The decision in the case of *District Registrar and Collector vs Canara Bank*[27], has significant implications for recognizing informational privacy, as it was held that an individual has a reasonable expectation that information provided to a third party will be used only for the purpose for which it was provided. In the case of *Hindustan Times v High Court of Allahabad*[28], the court stressed that the job of the media is to give information and viewpoints that have been tested and proven to be truthful and correct to readers and the broader public. In the case of *National Legal Services Authority vs Union of India*[29] the court held that Article 21, which speaks of the rights to life and personal liberty, is the heart and soul of the Indian constitution. Article 21 encompasses all elements of life that contribute to the purpose of a person's existence. Article 21 safeguards human dignity, personal autonomy, and the right to privacy, among other things. This decision explains why a right to privacy should be grounded in the protection of gender identity under Article 15. A basic right to privacy is formed at the intersection of Articles 15 and 21 as an expression of individual autonomy, dignity, and identity. Though a fundamental right to privacy is essentially

[25]X vs Hospital, (1998) 8 S.C.C. 296 (India).
[26]PUCL vs Union of India, (1997) 1 S.C.C. 301 (India).
[27]District Registrar and Collector vs Canara Bank,(2005) 1 S.C.C. 496 (India).
[28]Hindustan Times v High Court of Allahabad, (2011) 13 S.C.C. 155 (India).
[29]National Legal Services Authority vs Union of India, (2014) 5 S.C.C. 438 (India).

found in Article 21's guarantee of life and personal liberty, it is supplemented by the ideals included in other rights specified in Part III of the Constitution.

Finally, one of the most important judgement in Indian history which changed how right to privacy is to be viewed was delivered by a 9-judge bench wherein for the first time, right to privacy was conferred the status of fundamental right. It was in the case of *Justice K.S Puttaswamy (Retd.) vs Union of India &Others*[30] (hereinafter referred as Puttaswamy Judgement), where the court held that "*the right to privacy under Article 21 is safeguarded as an inherent aspect of the right to life and personal liberty, as well as one of the freedoms granted by Part III of the Constitution."* To shield an individual's private space from State and non-state intrusion, the right to privacy is considered as a yardstick that permits people to make autonomous life choices.

3.2. Analyzing different contours of Privacy as determined in the Puttaswamy Judgement

In Puttaswamy case, the judges were unified in their belief that privacy is the constitutional core of human dignity and autonomy. The unanimous results reached by the judges in this case show that privacy includes bodily integrity, the element of mind (self-determination), dignity, freedom, and independence, and is linked to the fundamental freedoms provided in Part III of the Constitution. Since it has been designated as a fundamental right, the State's involvement in ensuring the right is critical. The ruling of the case indicates that in future, it may so happen that many additional elements of privacy will be covered. In this case different connotation of privacy was discussed such as (i) spatial control; (ii) decisional autonomy; and (iii) informational control. The establishment of private areas is referred to as spatial control. Personal decisions such as reproduction, as well as public choices such as faith or what clothes to wear, are all covered under decisional autonomy. Individuals with informational control can utilize privacy as a barrier to maintain personal control over information about themselves. Privacy is a suitable safeguard against the unwanted circulation of personal data, according to the notion of informational control. It is critical to grasp what informational privacy is at this point, as the problem at hand is the preservation of informational privacy in cyberspace.

[30]Justice K.S Puttaswamy (Retd.)&Anr vs Union of India &Others,(2017) 10 S.C.C. 1(India).

3.3. Informational Privacy

We live in an information age, where even a small piece of information about someone can provide that person with significant power. Life has become inherently connected as a result of technological advancements. The internet is now all-encompassing as people continue to spend more time online on a daily basis. Internet is being used as a mode of communication for people to connect with each other. The internet is being widely utilized for conducting businesses and to purchase products as well as services. People use the internet to find information, send e-mails, use instant messaging services, and download movies. Today, popular websites install cookie files via the user's browser which may tag browsers with unique identifier codes, allowing companies to quickly recognize users and deduce information about online activities and habits.[31] Information, particularly a person's surfing history, is then used to construct user profiles. Algorithms enable the building of profiles relating to the internet users. A user's email is read by the help of automated content analysis of the emails. This may be done to determine user's interests and preferences, which in turn helps to tag appropriate commercials and advertisements to a user on their browser window. Electronic surveillance is being used to monitor people's lives. The right to privacy is jeopardised when information is utilised for a completely different reason other than the actual reason for which it was departed. Individuals are not always notified that other persons have access to the information that belongs to them, and this exclusion violates their right to informational privacy. The ability of a person to manage the use of his information is a necessary aspect of the right to privacy.[32]

Informational privacy represents a desire to keep personal information from being exposed. Here, the notion of "informed consent" becomes extremely significant.[33] Data distribution is regarded as one of the most serious misconducts of privacy since it deprives a person of his or her right of self-determination. Data manipulation and its

---

[31] Guido Noto La Diega, *The Internet of Citizens: A Lawyer's View on Some Technological Developments in the United Kingdom and India*, 12 Indian Journal of Law and Technology 53 (2016).

[32]Bernard A. Berkman, *The Assault on Privacy: Computers, Data Banks, and Dossiers, by Arthur R. Miller*, 22 CASE W. RSRV. L. REV. 808 (1971). Available at: https://scholarlycommons.law.case.edu/caselrev/vol22/iss4/10.

[33]Vrinda Bhandari & Renuka Sane, *Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018*, 14 Socio-Legal Review 143 (2018).

usage without the approval of the person inhibits decision-making. When it comes to the creation of a data protection regime, which is a complicated task in itself, the State must carefully balance the individual privacy interests on one hand and the legal concerns of the State on the other.[34] Concerns about national safety must be taken into account when formulating a data protection policy. The reason being that today cyberspace is used for various illicit activities such as hackers can take advantage of the web's seamless architecture to create havoc on the civilized nations.[35]

Though it is held that right to privacy is fundamental right under Article 21 of the Constitution, it is not an absolute right. A law that infringes on privacy must pass the test of constitutionally acceptable limits on fundamental rights. In the framework of Article 21, an invasion of privacy must be justified by a legislation that specifies a fair, just, and reasonable method.[36] This right is subject to reasonable State limitations designed to safeguard genuine State or public interests. One such genuine State interest would be national security. Furthermore, when it comes to limitations on this right, the provisions of several articles under Part III of the constitution that correspond to the right must be scrupulously followed.

3.4. Scope of limitations on the Right to Privacy

Like any other right, a person's privacy is subject to reasonable limitations. When the government monitors the internet to protect the country from cyber-attacks and terrorist operations, it has a legitimate interest. While intervening to safeguard legitimate State interests, the State must also put in place a rigorous framework that guarantees that a three-fold requirement is met. This three-fold test is enumerated in the Puttaswamy judgment and it applies to all privacy restrictions, not only informational privacy restrictions. The first requirement that there must be a law in existence, second, a legitimate aim of the State and third, it should be proportionate i.e., there must be a rational nexus between the goals and the methods used to attain them. In this context, the term 'legitimate aim' refers to a law's purpose that is rational, constitutionally lawful, and does not contain any element of manifest

[34]Varun Kalra, and Ramisha Jain, *An Armistice between Right to Privacy and Right of Surveillance*, 4 INDIAN JOURNAL OF LAW & PUBLIC POLICY 1-23 (2017).
[35]Dhiraj Kukreja, *Securing Cyberspace*,2 LIBERAL STUDIES 59-68, (2017).
[36]*What Fundamental Right to Privacy means and what it doesn't: 10 points from Supreme Court verdict*, Financial Express, August 24th, 2017, https://www.financialexpress.com/india-news/what-fundamental-right-to-privacy-means-and-what-it-doesnt-10-points-from-supreme-court-verdict/823334/

arbitrariness. Proportionality is an important aspect of the protection against arbitrary State action since it guarantees that the nature and quality of the infringement on the right are not out of proportion to the law's objective. As a result, the reciprocal interdependence of the basic safeguards against arbitrariness on the one hand, and the protection of life and personal liberty on the other, gives birth to the threefold requirement for a legitimate legislation.

Individuals' privacy worries have grown in the modern world as data has become more digitalized. There are a variety of players involved in the procedure of information accumulation, processing, and distribution at multiple levels. During this process, it is most likely that the data might be exploited for illicit motives. Further, economy's reliance on IT has grown considerably over time. Therefore, there is extremely necessary to devise a robust data protection policy. Cyber law acts as a shield over cyberspace thus prevent any kind of cybercrime from happening. Cyber law covers matters relating to intellectual property, contract law, data protection regulations, as well as privacy related issues. Countries all around the world are enacting stronger data protection regulations in order to combat data theft. In India, the IT Act of 2000, as well as IT Rules thereunder, come to the rescue in terms of safeguarding personal data. The following chapter discusses how IT Act protects individual data by analysing some of the key provisions of the IT Act and the relevant rules under it.

CHAPTER IV

4. COMPREHENDING RELEVANT PROVISIONS OF THE IT ACT AND IT RULES

4.1. Relevant Data Protection Provisions Under IT ACT

The IT Act was enacted with the intention of providing legal recognition for transactions involving electronic data exchange and other types of electronic communication, colloquially known as "electronic commerce" which entails the use of non-paper-based methods of communication and data storage. It is India's primary privacy regulation, along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(*hereinafter referred as Privacy Rules*).[37] Some other acts where traces of privacy can be located are: the Indian Penal Code, 1860; the Indian Telegraph Act, 1885; the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; and the Protection of Children from Sexual Offences Act, 2012 etc.The IT (Amendment) Act 2008 was passed, which included, among other things, the addition of two new sections to the IT Act, Sections 43A and 72A, which govern incorrect disclosure of personal information.[38]

Section 43A creates a mandatory data protection system that requires implementation of "appropriate security policies and procedures" in connection to any sensitive personal data or information handled by a body corporate. If there is a failure to secure data, then the body corporate will be liable to compensate the affected person. Despite the fact that Section 43A requires a body corporate to pay compensation for any negligence in maintaining reasonable security practises and procedures that results in loss, it does not prescribe any criminal penalty, even if there is intentional failure to maintain reasonable security practises and procedures.[39]

---

[37]Rachit Bahl, Aprajita Rana & Aman Gera, *Q&A on Data Protection and Cybersecurity*, (May 11th, 2020), https://www.azbpartners.com/bank/qa-on-data-protection-and-cybersecurity/

[38] Aditi Subramaniam &Sanuj Das, *In a nutshell: data protection, privacy and cybersecurity in India*, LEXOLOGY, (October 22, 2020), https://www.lexology.com/library/detail.aspx?g=04c38a97-f6cb-4d23-ae95-00df33df8a68.

[39] Vinod Basu, Protiti Base &Ashwarya Bhargava, *A Review of the Information Technology Rules, 2011 Reasonable Security Practice and Procedures and Sensitive Data or Info,* MONDAQ, (MARCH 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-.

Even though individuals can seek compensation from body corporates under Section 43A, it is the Privacy Rules under it which imposes additional important obligations such as obtaining consent, processing for a restricted purpose, preserving only for as long as necessary, and sharing only with prior consent. However, it applies only to sensitive personal data such as passwords, health data, financial data, or biometrics not personal data in general.[40]

In the case of a breach of a valid contract, Section 72A of the IT Act safeguards personal information and specifies the penalties for any disclosure of information with the goal or knowledge of causing wrongful loss or wrongful benefit.[41]The penalty would be imprisonment for a maximum of three years or a fine of up to five lakh rupees or both. However, a body corporate may have a larger turnover and hence the penalties levied in the event of a data breach will be a meagre amount, and they may be able to get away with it.

Section 69 of IT Act deals with legal mechanisms that helps in cyberspace surveillance and interception.[42] Under this provision, the government is given authority to intercept, monitor, decrypt, and restrict online content provided it is required in the interests of state security, public order, India's sovereignty and integrity, and so on. When an order is granted under this section, the grounds must be specified in writing. The Central Government framed the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 under Section 69 read with Section 87 of the IT Act. It was enacted to provide checks and balances as well as procedures for interception. To ensure that privacy is not inadvertently breached, such interception requires prior authorization from the appropriate authorities. Specifically, the Secretary in the Ministry of Home Affairs in the case of the Central Government and the Secretary in charge of the home department in the case of the State Government.[43]

The current surveillance regime puts all authority in the hands of the executive, necessitating urgent reform, i.e., the necessity for judicial scrutiny.[44] Despite existing

---

[40] Siddharth Sonkar, *Privacy delayed in privacy denied*, The Wire, May 24th, 2021, https://thewire.in/tech/data-protection-law-india-right-to-privacy

[41]NS NAPPINAI, TECHNOLOGY LAWS DECODED, (1st Edition, Lexis Nexis), 2017

[42]Section 69 of the Information Technology Act, 2000.

[43]Rule 3 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[44]*IFF files rejoinder in PIL seeking surveillance reform*, INTERNET FREEDOM FOUNDATION, 23rd April, 2019 https://internetfreedom.in/iff-files-rejoinder-in-pil-seeking-surveillance-reform/.

rules and regulations, the government is finding it more difficult to have them enforced as many corporations do not have a physical presence inside India's territorial jurisdiction. Global messaging businesses like as WhatsApp and Telegram argue that because their systems are end-to-end encrypted and the private keys are stored on the user's phone/computer, it is difficult to intercept the content of individual users' messages. The government needs to work for a formulation of a workable and suitable encryption policy.[45] The expansion of e-commerce should be aided by providing appropriate tools to protect privacy in cyberspace. It is critical to keep the online medium reasonably safe for users so that any personal information they provide stays private and users' privacy rights are honoured.

4.2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

In 2011, under Section 43A of the IT Act, India formalized individual's right to protect personal information by enacting the Reasonable Security Practices and Procedure for Sensitive Personal Data or Information Rules.[46] The Privacy Rules specify the processes and protocols that must be followed by body corporates which are then required to implement appropriate security practises including comprehensive information security programmes and policies. The Privacy Rules defines personal information and sensitive personal data/information separately.[47] Passwords, financial information, sexual orientation, medical records, and biometric information are some of the examples of sensitive personal information. It also states that publicly available information will not be deemed as sensitive personal data.[48] The Privacy Rules give data subjects specific rights, such as the ability to review their data, the ability to refuse or withdraw consent, the requirement that data be collected for legitimate purposes, and the restriction that data be kept for no longer than is

[45]NS Nappinai, *Supra* note at 41.
[46]Bhairav Acharya, *Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, THE CENTRE FOR INTERNET & SOCIETY, 31st March, 2013, https://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.
[47]Rule 2 (i) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[48]Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

necessary.[49] The Privacy Rules, on the other hand, place no requirement on the body corporate to notify such rights to the information providers.[50] The legislation also requires that the provider of sensitive personal information to give their consent, however in today's world, where data is collected from many sources, the manner in which consent is obtained is difficult to comprehend.[51] Furthermore, a user may not even be aware of when he or she consented to be tracked and given information when everything happens with a single click. From monitoring our call records to tracking our movement and surfing history, privacy can be undermined by a single act or multiple acts by gathering and profiling information, both by the State and private actors.

4.3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Recently, a new set of Intermediary Rules was issued by the government, i.e., The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (*hereinafter referred as Rules 2021*).[52] It superseded the former Information Technology (Intermediaries guidelines) Rules, 2011. The Rules 2021 have been formalized at a time when the nation is relentlessly making an effort to safeguard cyberspace safety and sovereignty and to protect personal data of individuals. Since its introduction, this rule has been criticised heavily. It is argued that the present version of the rule lacks a cogent reasoning and goes beyond the perimeters of the parent statute.[53] Additionally, the wordings in the rule are vague, and intermediaries are subject to arbitrary obligations of content control, traceability,

[49]Rule 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[50]Rachit Bahl, *Supra* note at 37.
[51] Kritika Bhardwaj, *Preserving Consent within Data Protection in the Age of Big Data*, 5 NATIONAL LAW UNIVERSITY DELHI STUDENT LAW JOURNAL 100-110 (2018).
[52]*Government notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, PRESS INFORMATION BUREAU, GOVERNMENT OF INDIA, MINISTRY OF ELECTRONICS & IT, February 25th, 2021 https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1700749.
[53]*Why The Wire wants the new IT rules struck down*, The Wire, March 09th, 2021, https://thewire.in/media/why-the-wire-wants-the-new-it-rules-struck-down

and decryption.[54] This not only jeopardizes the freedom of speech and expression, but also the Right to Privacy of those who utilise these services.[55]

Part of this regulation is inspired by Section 79 of the IT Act, which offers a "safe harbour" by which it frees the intermediaries from obligation for the content posted by their customers on the intermediaries platforms, provided they adhere to the liabilities and regulations under the Act and the related Rules.[56] We are at a point in time when social networking platforms are progressively becoming an essential component of a person's daily routine. Tech companies can't overlook the emerging and unprecedented issues such as rise in circulation of fake news, unrestrained exploitation of social media networks to disseminate altered pictures of women etc. In this context the new Rules 2021, provide measures that strengthen the accountability of intermediaries and safeguard consumers.[57]

The main point of discussion is Rule 4 (2) of Rules 2021, which compels significant social media intermediaries to recognize and reveal the "first originator" of information for prevention, detection and investigation of an offence. This rule is being argued to be a serious invasion to the right to privacy. A social media intermediary must have fifty lakh registered users in India to be designated a significant social media intermediary, according to a government notification.[58] When it comes to traceability orders, the Rules 2021 make it clear that they are reserved for grave violations and infringements, however there are some categories that are still undetermined. For example, "public order" as one of the grounds under Rule 4(2) is comparatively wide and there is no way to ascertain which message would violate public order that government would want to investigate. As per Rules 2021, social media intermediary is not obligated to reveal the details about any electronic message,

---

[54]*Deep dive: How the intermediaries rules are anti-democractic and unconstitutional,* INTERNET FREEDOM FOUNDATION, February 27th, 2021, https://internetfreedom.in/intermediaries-rules-2021/.

[55]*IFF Releases Legislative Brief on Digital Rights for the Monsoon Session of the Parliament, Internet Freedom Foundation,* INTERNET FREEDOM FOUNDATION, July 24th, 2021, https://internetfreedom.in/iff-releases-legislative-brief-on-digital-rights-for-the-monsoon-session-of-the-parliament/.

[56]Section 2 (w) of the Information Technology Act, 2000.

[57] Namrata Maheshwari & Emma Llanso, *Part 1: New Intermediary Rules in India Imperil Free Expression, Privacy and Security*, CENTER FOR DEMOCRACY & TECHNOLOGY, May 25th, 2021, https://cdt.org/insights/part-1-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/.

[58]Ministry of Electronics and Information Technology Notification dated February 25th, 2021, https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf

as well as any other information linked to the initial originator or other users.[59]But the IT Decryption Rules, 2009 on the other hand, provide the government the authority to demand the communication of content.[60] To find out who transmitted what content and what did it contain, the government can make use of these two tools jointly. Such a measure disrupts current procedures and protocols for the implementation of end-to-end encryption, which have been established over the years by extensive cyber security testing. This traceability requirement has significant implications, as can be seen in the IT Decryption Rules, 2009, where there is no effective judicial check on monitoring, and with this latest Rules 2021 will give the government enormous influence and advantage.[61]

Some argue that the requirement for traceability is incompatible with the use of services such as WhatsApp that provide users with the freedom to communicate and express themselves while knowing that their communications are protected from unauthorised access and can only be read by those who are supposed to receive them (end-to-end encryption). It is been argued that end-to-end encryption is a component of the basic right to privacy recognised in Puttaswamy Judgement, and the Intermediary Rules, 2021 attempt to undermine it.[62] Traceability, no matter how it is done, will either significantly degrade or break encryption, resulting in the loss of anonymity, privacy, and free expression. There is also no requirement for any prior judicial review when it comes to the government ordering the revealing of identity.[63] Tracking of initial originator is seen as a fair constraint on the fundamental right of privacy by government officials.[64] Further, knowing the "first originator" of information of messages that incite violence, rioting, terrorism, rape, or a threat

[59]Rule 4 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

[60]Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Notification dated October 27th, 2009, New Delhi, https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf.

[61]*Latest Draft Intermediary Rules: Fixing big tech, by breaking our digital rights?*,INTERNET FREEDOM FOUNDATION, February 25th 2021, https://internetfreedom.in/latest-draft-intermediary-rules-fixing-big-tech-by-breaking-our-digital-rights/.

[62]Praveen Arimbrathodiyil vs. Union of India, W.P.(Civil) 18084 of 2021 (India).

[63] Namrata Maheshwari & Greg Nojeim, *Part 2: New Intermediary Rules in India Imperil Free Expression, Provacy and Security*, CENTER FOR DEMOCRACY & TECHNOLOGY, June 04th, 2021, https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/.

[64] Anil Sasi & Pranav Mukul, *WhatApp vs. Govt: The two cases in HC, each side contradicts itself*, The Indian Express, June 07th, 2021, https://indianexpress.com/article/india/whatsapp-vs-govt-delhi-high-court-privacy-policy-update-7347103/.

to national security falls within justifiable exceptions to the Right to Privacy - which, as the Constitution states, is not absolute.[65] The government further highlighted that Rule 4(2) meets the proportionality test since the originator of the information is to be tracked in instances where alternative remedies have proven ineffectual, making it a last resort measure.[66] The impact of Rules 2021 on major IT corporations will only be known over time, as the new Rules 2021 are currently being challenged in various Indian courts on various grounds.[67]

WhatsApp has filed a case in the Delhi High Court against the government, arguing that the Rules 2021, requiring significant social media intermediaries to offer traceability of the first originator of unlawful conversations, are a substantial invasion of user privacy.[68] The origin of a message may potentially be traced by providing information such as the sender's phone number, time the message was sent, device from which it was sent etc. It is also being argued that breaking the encryption might put groups like journalists, human rights campaigners, and political activists at risk. Hence, complying with the requirement of traceability when requested by authorities would result in the breaking of end-to-end encryption by compelling messaging services to trace chats, which is equal to keeping a fingerprint of every single message transmitted thereby putting users' privacy at risk.[69] Only "extremely grave offences" that undermine India's sovereignty and integrity will require traceability, according to the government. As an added bonus, it can be done without jeopardising end-to-

[65]Sidhartha and Pankaj Doval, *Rules protect rights of users, were framed because social media giants failed to do so: IT and law minister Ravi Shankar Prasad*, The Times of India, June 01st, 2021, https://timesofindia.indiatimes.com/india/rules-protect-rights-of-users-were-framed-because-social-media-giants-failed-to-do-so-it-and-law-minister-ravi-shankar-prasad/articleshow/83128246.cms.

[66]*Whatsapp challenges intermediary Rules, says traceability will break end-to-end encryption, breach privacy; Union of India says no Fundamental Right is absolute*, SCC Online, May 27th, 2021, https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/

[67]*Union of India seeks a transfer of cases challenging IT Rules*, 2021, Internet Freedom, https://internetfreedom.in/union-of-india-seeks-a-transfer-of-cases-challenging-it-rules-2021/

[68]Debopama Bhattacharya, *The Information Technology (IT) Rules, 2021*, MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES, June 04th, 2021, https://www.idsa.in/idsacomments/it-rules-2021-dbhattacharya-040621#footnote1_s0qthit.

[69]Joseph Menn, *WhatsApp sues Indian government over new privacy* rules, Reuters, May 26th, 2021, https://www.reuters.com/world/india/exclusive-whatsapp-sues-india-govt-says-new-media-rules-mean-end-privacy-sources-2021-05-26/

end encryption. However, companies will be responsible for developing a technical solution to the problem.[70]

Interestingly, there is another case where in WhatsApp's new privacy policy which allows it to share user metadata with Facebook, for tailored advertisements.[71] The WhatsApp has been given notice by the Union Government to withdraw its new privacy policy, claiming that by requiring users to agree and assent to the policy, it is engaging in anti-user practices whilst Personal Data Protection Bill 2019 is still pending.[72] WhatsApp's privacy policies which is now on hold jeopardise the sacrosanct principles of informational privacy.[73] Due to the General Data Protection Regulation (GDPR), which shields consumers from sharing their data with Facebook and provides them the freedom to decline WhatsApp's new terms of service, European WhatsApp users have the option of opting out. When individuals want companies to know less about them, a policy such as this allows companies to learn more about its users. Another reason to consider a strict data protection law in India.[74] Since, all these cases are pending in the Court, the outcome would be a real-world test of how to defend one's fundamental right to privacy in an era marked by rapid technology advancements.

As long as the Constitution has been in place, finding the right balance between fundamental rights and the rationale of a limitation has been a constant challenge for lawmakers. The conversation has now shifted to the digital sphere. Until optimal solutions can be found, the ongoing battle between private tech giants that own significant amounts of big data, governments that want to impose reasonable restrictions, as well as users concerned about data privacy and restrictions on freedom of speech and expression, will only become more complex. Both the government and digital intermediaries have used every chance to argue that they are the biggest supporters of people's right to privacy, which the

[70]Debopama Bhattacharya, *Supra* note at 68.
[71]Anil Sasi, *Supra* at 64.
[72]*Centre asks WhatsApp to withdraw 'discriminatory privacy policy, gives 7days to respond*, The Week, May 19, 2021, https://www.theweek.in/news/biz-tech/2021/05/19/centre-asks-whatsapp-to-withdraw-discriminatory-privacy-policy-gives-7-days-to-respond.html.
[73] Kaushik Deka, *The battle for online privacy*, India Today, June 11, 2021, https://www.indiatoday.in/magazine/special-report/story/20210621-the-battle-for-online-privacy-1813369-2021-06-11.
[74]Nandana James, *WhatsApp's new privacy policy: Yet another reason why India needs data protection law*, Business Line, January 10,2021, https://www.thehindubusinessline.com/info-tech/whatsapps-new-privacy-policy-yet-another-reason-why-india-needs-data-protection-law/article33542521.ece.

Supreme Court has proclaimed a fundamental right. However, in this domain of 'virtual' conversation, the user must not become a victim in this game of one-upmanship over who controls the remote. The requirements for intermediaries are pretty clear: if the government wants data, it only needs to ask the intermediary, and they must supply it. In this all discussion and debate, we must not forget that the data belongs to the individuals, not the intermediaries.[75]

The IT Act and the rules framed thereunder till now have protected data but given the limited scope of the erstwhile data protection rules coupled with the increased use of data and the internet, it has become clear that a comprehensive legislation protecting people's fundamental right to privacy is required which is still missing in India. We need a structured and dedicated legislation dealing with data protection like the EU's General Data Protection Regulation (GDPR). In order to build a free and fair digital economy that respects an individual's privacy rights, India is working on its much-anticipated data protection law, The Personal Data Protection Bill, 2019 (Bill 2019). This Bill 2019 is yet to be passed.[76] The following chapter discusses the key provisions of the Bill 2019 and EU's GDPR. It will also examine whether India will benefit from EU-style data protection and finally what strategy could be adopted in resolving the problems related India's data privacy regime.

[75]Prasid Banerjee & Richa Banka, *WhatsApp case in Delhi HC first big test of privacy law*, Mint, May 27th, 2021, https://www.livemint.com/news/india/whatsapps-case-against-indian-govt-could-be-first-true-test-of-right-to-privacy-11622028707630.html

[76] Neha Alawadhi, *Personal data protection bill JPC gets new chief in P P Chaudhary*, Business Standard, July 22, 2021, https://www.business-standard.com/article/current-affairs/personal-data-protection-bill-jpc-gets-new-chief-in-p-p-chaudhary-121072201429_1.html.

CHAPTER V

5. ANALYSING PERSONAL DATA PROTECTION BILL, 2019 AND EU'S GENERAL DATA PROTECTION REGULATION

5.1. Personal Data Protection Bill, 2019

The bill owes its origin to the landmark case on data privacy, the *Puttaswamy Judgement*. The Government of India established an expert group in 2017 under the head of retired Justice B. N. Srikrishna to study data protection concerns and develop a comprehensive data protection policy.[77]The committee produced a draft Personal Data Protection Bill in in the year 2018which was amended and the new Bill 2019 was approved by the cabinet. The PDP Bill 2019 is modelled after the GDPR and aims to revamp India's present data protection law, which is currently governed by the IT Act of 2000 and its rules thereunder.[78] The Bill 2019 has put a number of restrictions on data processing, with the premise that the average person would have little understanding of how their data is processed.

The Bill 2019 states that data collected should for specific, clear, and lawful purposes[79] which should be in a fair and reasonable manner.[80] The Bill 2019 envisages for the creation of a Data Protection Authority (DPA), whose mission will be to prevent the abuse of personal data and guarantee that the Bill's provisions are followed.[81] The data has been categorized into three categories (i) personal data[82], (ii) sensitive personal data[83] and (iii) critical personal data. However, the central government would notify the definition of critical personal data.[84] It also contains provision with respect to data localization wherein data fiduciaries will have to store data in India.[85]Various novel concepts have also been introduced such as creation of

[77]Anurag Vaishnav, *The Personal Data Protection Bill, 2019: All you need to know*, 2019, PRS Legislative Research, December 23rd, 2010, https://www.prsindia.org/blogcomment/844671.
[78]Purushotham Kittane, Inika Serah Charles, Aaron Kamath & Gowree Gokhale, *Privacy and Data Protection-India Wrap* 2020, The National Law Review, Volume XI Number 244, September 1st, 2021, https://www.natlawreview.com/article/privacy-and-data-protection-india-wrap-2020.
[79]Section 4 Personal Data Protection Bill, 2019.
[80]Section 5 Personal Data Protection Bill, 2019.
[81]Section 41 Personal Data Protection Bill, 2019.
[82]Section 3(28) Personal Data Protection Bill, 2019.
[83]Section 3(36) Personal Data Protection Bill, 2019.
[84]Section 33(2) Personal Data Protection Bill, 2019.
[85]Rishab Bailey, *The issues around data localisation*, The Hindu, February 25th, 2020), https://www.thehindu.com/opinion/op-ed/the-issues-around-data-localisation/article30906488.ece.

sandbox[86], creation of privacy by design policy[87] has been introduced.[88] Even though this is India's first comprehensive data protection bill if enacted would be beneficial to crores of Indian citizens, it is still not free from criticisms. The PDP Bill, 2019, creates extensive carve outs for anonymised non-personal data, as well as sandboxes that might jeopardise individuals' privacy rights due to a lack of consent. Another major flaw in the PDP Bill 2019 is the lack of independence of the DPA's selection board, which is made up entirely of government officials with no representation from the judiciary, opposition, or civil society. This is significant because the DPA was established to protect persons from both corporate and government institutions. Furthermore, Bill 2019 authorises the Central Government to issue a written order exempting "any agency" of the government from all or parts of the data protection law.[89] It vests power in the central government and clearly designates it as the judge and arbitrator in its own case. The majority of India's intelligence services lack institutional control, and there are no laws that explicitly define their capabilities and restrictions.[90] In addition, the Bill contains no real examination of telephone tapping and other communications interception powers. This will expose citizens personal data to mass surveillance, rendering protection ineffective.[91]The Bill 2019 also makes no provision for data collected previous to the Bill's enactment, and it contains no transitional provisions.[92]Despite its flaws, the Bill 2019 is a long-awaited and unquestionably good move in the right direction. Hopefully, all the stakeholders involved in passing the Bill will fill up the gaps and give the country a strong data protection law, which is urgently needed.

---

[86]Section 40 Personal Data Protection Bill, 2019.
[87]Section 22 Personal Data Protection Bill, 2019.
[88]Arun Prabhu, *The Personal Data Protection Bill 2019, An Analysis*, INDIA CORPORATE LAW, A CYRIL AMARCHANDMANGALDAS BLOG, December 12th, 2019, https://corporate.cyrilamarchandblogs.com/2019/12/personal-data-protection-bill-2019-analysis-india/#_ftn1.
[89]Section 35 Personal Data Protection Bill, 2019.
[90]*Watch the Watchmen Series Part 5: The Personal Data Protection Bill, 2019*, Internet Freedom, October 28th, 2020, https://internetfreedom.in/watch-the-watchmen-series-part-5-the-personal-data-protection-bill-2019/
[91]Probir Roy Chowdhury, YajasSetlur& Kavya Katherine Thayil, *Why data privacy must be safeguarded, even in times of COVID-19*, FINANCIAL EXPRESS, May 19th, 2020, https://www.financialexpress.com/money/why-data-privacy-must-be-safeguarded-even-in-times-of-covid-19/1963579/.
[92] *Save our Privacy, A public brief and analysis on the Personal Data Protection Bill, 2019*, Internet Freedom Foundation, https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf

5.2. European Union General Data Protection Regulation

The EU's GDPR, which took effect on May 25, 2018, is widely regarded as a watershed legislation for the protection of citizens' data privacy.[93] All organisations that process personal data of EU citizens, regardless of location, are subject to the GDPR.[94] Because of its unique characteristics, such as the right to erasure and breach notification rules, it is of worldwide importance. It is one of the comprehensive rules that has made the EU's interpretation and enforcement consistent. The GDPR also includes a data protection certification process, as well as data protection seals and markings, to guarantee that data controllers comply with the Regulation when transferring data internationally.[95] The GDPR addresses the issue of personal harm caused by automated decision-making stating that a data subject has the right to object to the use of personal data for marketing purposes. It is worth noting that GDPR does not include a need for data localization.[96] The data subject has a number of privacy rights under GDPR, including the right to be informed, the right to data portability, the right to be told about automated decision-making and profiling, and the right to rectification, to mention a few.[97]GDPR has been beneficial for both individuals and businesses, where in one hand it has increased the role of EU individuals in controlling data by making them feel more powerful and aware of their legal rights and protections, and on the other businesses viewed having an uniform set of laws to follow across the EU as a positive step.

---

[93] European Union, What is GDPR, the EU's new data protection law?,*available at*https://gdpr.eu/what-is-gdpr/.

[94]Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019,* Digital Guardian, September 30th, 2020, https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

[95]Manya Gupta & Sunanda Tewari, *Tipping the Scale: Weighing Personal Data Protection Bill, 2019 against EU's GDPR*, First Post, December 18th, 2019, https://www.firstpost.com/tech/news-analysis/tipping-the-scale-weighing-personal-data-protection-bill-2019-against-eus-gdpr-7796161.html.

[96]Anirudh Burman & Upasana Sharma, *How would Data Localisation Benefit India?,* Carnegie India, April 14th, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

[97]Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/

5.3. Analysis

While GDPR appears to be a model for the PDP, however there are differences that distinguish the it from Bill 2019. Countries that have particular laws protecting personal data would definitely be in a better position. When designing its own personal data protection regulations, India can turn to Europe for inspiration, but only those that are most suited to the Indian context should be implemented. The first thing to do is to understand and analyse how our legal system works because India is a distinct and diverse country with its own unique social, political, and economic structure. It is not always practical to transplant a country's legal system to another; after all, it is hard to predict how a law will operate once it has been passed. There are provisions in Bill 2019 which are similar to that of GDPR and hence it should be modified to the extent it can meet the realities of India economy. As the global data protection environment becomes more intricate, a thorough analysis of the standards in each jurisdiction will be essential and beneficial.

CHAPTER VI

6. CONCLUSION AND SUGGESTIONS

Cyberspace is currently undergoing unprecedented development and turmoil. The technology is advancing at lightning speed; newer innovations and enhancements emerge even before the current ones have settled and stabilized. The internet proved to be an effective battlefield for cyber-attacks and psychological warfare by both state and non-state actors due to a lack of stringent legislation. There is a large amount of personal information exchanged via the internet as a result of technical advancements and increased usage. Humans have benefited from the use of these technologies in a variety of ways, including the ability to communicate more quickly, improve education, etc. However, all of this has come at the detriment of privacy. The necessity for privacy over certain information is controversial, as some indirect information acquired may be useful to an organisation for advertising purposes but may be inconsequential to an individual. Currently, the majority of cyber world is controlled and governed by a limited group of big corporations that have global commercial interests. It is proving to be quite difficult for the States to govern and protect an ever-expanding realm that is global in essence and is run by giant tech firms having a spatially separate existence. Further it is proving to be complicated for them to substitute a global technology or application with a domestic equivalent, given the immense magnitude of the technical and economical challenge. Due to the rapid advancement in this realm and outdated instruments with the state, the edge is always with that smaller section of individuals and organizations those are quite proficient in this area.

In India, cyberspace has proven to be extremely beneficial. As a country, we have never seen a real leveller that seems to be able to bridge the gap between the wealthy and poor, as well as between the privileged and the disadvantaged. It has freed our dormant inventiveness, intellectual power, business acumen, and governance from their shackles. With the introduction of the internet, cyber-crime and cyber-attacks have also exploded. During the initial stages of the internet, cyberspace security was given relatively little thought, as most of the emphasis was given to expanding network connectivity with minimal cost with regard to software, speed of processing, data cost and memory. Therefore, the hackers during the early days got succeeded in

exploiting this vulnerability to cause interruptions, distortion, and damages. As the internet grew in popularity and provided ways leading to additional sectors such as e-commerce, e-finance, and media platforms, cyber-crime grew massively, prompting governments to establish multi-layered security systems and structures to combat the problem.

The Indian surveillance architecture has two flaws: the first is the broad mandate provided to law enforcement authorities, as well as the lack of judicial or independent supervision. The second point to consider is state capacity. In terms of the amount of surveillance requests filed, the choice to place persons under surveillance is largely discretionary.[98] Given the power imbalance between citizens and governments, the only effective way to limit government action is to enact a comprehensive law that restricts what the government can do, defines the circumstances in which it may infringe on fundamental rights, regulates law enforcement agencies, establishes control and oversight mechanisms, and empowers citizens to hold the government accountable.

We've come a long way in terms of how the courts viewed privacy, from just mentioning it is as a passing reference to finally elevating it to the rank of a fundamental right in the Puttaswamy judgement. Having stated that, we must wonder why, even after so many years since privacy was recognised as a fundamental right, we still do not have any direct and comprehensive legislation dealing with data protection. Today, several significant draft legislations are being examined by the government, with delays that might last for months or even years before they are eventually passed into law. Newer legislations should be introduced in the same manner as technical developments. In addition to costing people and the government, every delay in enforcing enabling legislation gives intermediaries extra time to maximize revenue without fearing any legal repercussions. A number of digital partners have rapidly recognized that there is indeed a policy deficit relating to cyber data privacy protection. As a result of this deficit, a number of stakeholders are benefiting by taking initiatives that intends to get accessibility to citizen's data. A clear example of this is the newly revised WhatsApp privacy policy which was recently amended.[99]

[98]Vrinda Bhandari, *Supra* note at 33.

[99]Pavan Duggal, *Cyber data privacy in peril*, The Tribune, January 20th, 2021, https://www.tribuneindia.com/news/comment/cyber-data-privacy-in-peril-200925.

A major segment of our population is at a risk of falling victim to fake news, cybercrime/frauds, financial frauds and also giving consent to access information because of low literacy level, lack of awareness and information asymmetry. Rising awareness and educating public is essential at this point in time. In EU, GDPR was deemed effective as a result of greater awareness about it. Cyber hygiene, safe cyber activities, and cybercrime education should be mandated in all schools. Educating individuals on the need of protecting their private information is essential to their well-being. For this, behavioural changes are surely needed. The government, civil society groups, and professionals should not only enlighten the public through textual materials, but also ensure that the public understand their fundamental rights. Considering that internet access is not just available in India's urban regions, but also in the rural areas, this campaign must also reach the rural population. There is a significant number of cybercrimes that go undetected or are not prosecuted including fake news, financial fraud, sexual harassment, and molestation, due to a variety of reasons. Hence, there is a necessity to guarantee that any cybercrime that occurs in the nation may be reported easily and dealt with promptly.

Cyberspace is a dynamic environment that requires frequent re-examination and amendments to the cyberspace legislation. We need to maintain a law that achieves an appropriate balance between the need for individual's right to privacy, as well as businesses and government's demands for data for their respective legitimate interests. The largest collectors, manipulators, keepers, and users of data are bureaucracies and businesses. Individual privacy rights sometimes clash with the legitimate needs of governmental entities for individual data as public policy becomes increasingly data-centric. Although, data is acquired for creating products that aid in better prediction required to serve the users' needs, this violates the user's privacy, as this is done without their permission or acknowledgement. In our increasingly networked and digital society, there is an information asymmetry between the individual consumer and the data collector, which is widening. Individuals are unaware of the types of data collected about them or how it is used. This situation becomes even more problematic as data is used for secondary uses that were not initially intended, and several players (for collecting, preservation, consolidation, processing, and marketing) are involved, resulting in increased asymmetry. Furthermore, due to their incapacity to understand and interpret the fine print of privacy, individuals are unable to take rational decisions about the exposure of their

personal data. A law must be passed that strikes a careful balance between an individual's right to privacy and the governments and corporations genuine demands for data to serve them better. Rather than allowing the executive branch to utilise this data directly, the judicial intervention might be useful to control excessive authority in the hands of government. should approve an application for its use. Steps should include describing how data will be acquired, used, and disposed of after it has been used. As a result of these steps, various departments of the government will be able to maintain accountability and lucidity. Punitive measures should be handed out quickly for any infractions, and the Appellate Tribunal should be prompt in its decisions. IT companies should be more mindful of their procedures and make efforts to improve their data management and security configurations.

Today, although our government is making strides in the right way, there are still certain flaws that need to be rectified as quickly as possible in order to safeguard the privacy of individuals.

The Bill 2019 is a significant step forward in giving the right to privacy meaning and establishing a strong data protection framework for India. This Bill 2019 suffers from few infirmities hence steps should be taken to restore the true essence for which it was drafted. That being said, we are at a watershed point in history, on the verge of enacting a privacy law that will impact the lives of over a billion people. For privacy reform to be effective, it must be complemented by advances in state capacity.

The need of the hour is for a legislative framework that identifies concrete damages and develops solutions that take into account technology elements and privacy implications. Apart from adapting for a vigorous legislation, we also need stringent supervision and enforcement mechanisms while keeping in the mind the legality, necessity and proportionality tests. It is difficult to illustrate the negative consequences of losing one's privacy. Others should not be expected to preserve their personal interests or privacy. Such kind of maturity, in a developing democracy such as India, will take decades to become apparent to the general people. Much can be written and documented about the cyber domain, but one thing is certain: it is the domain of the future, and mastery of it is critical for a state's well-being and sustenance.

BIBLIOGRAPHY

BOOKS

1. M.P. Jain, Outlines of Indian Legal and Constitutional History (Lexis Nexis 2014)
2. Ashish Chibbar, Navigating the Indian Cyberspace Maze: Guide for Policy makers,(2020 ed., KW Publishers)
3. NS Nappinai, Technology Laws Decoded, 1st ed, (Lexis Nexis 2017)
4. Apar Gupta, Commentary on Information Technology Act - Along with Rules, Regulations, Orders, Guidelines, Reports and Policy Documents, (Lexis Nexis,2016)

RESEARCH ARTICLES/BLOG POST/GOVERNMENT NOTIFICATION

1. Government notified Information Technology *(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,* PRESS INFORMATION BUREAU, GOVERNMENT OF INDIA, MINISTRY OF ELECTRONICS & IT, February 25th, 2021
2. Information Technology (*Procedure and Safeguards for Interception, Monitoring and Decryption of Information*) Rules, 2009, Notification dated October 27th, 2009.
3. Ministry of Electronics and Information Technology Notification dated February 25th, 2021
4. Ryder, Rodney D., & Ashwin Madhavan, *Regulating Indian Cyberspace - The Battle for Control in the New Media Version 2.0* (2009).
5. Sam Jossen, *The world's most valuable resource is no longer oil, but data*, The Economist, May 6th, 2017.
6. Atin Kumar Das, *Interface between Technology and Society: A Study of the Legal Issues*, 8 INDIAN JOURNAL OF LAW AND JUSTICE 120-127 (2017).
7. Umang Joshi, *Online Privacy and Data Protection in India: A Legal Perspective*, 7 NUALS LAW JOURNAL 95-111, (2013).
8. F Cassim, *Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves*. 18 POTCHEFSTROOM ELECTRONIC LAW JOURNAL 68-110 (2015).
9. Sougata Talukdar, *Privacy and Its Protection in Informative Technological Compass in India*, 12 NUJS L REV 287 (2019).

10. Frackman, Andrew J., and Martin, Rebecca C., *Surfing the Wave of On-Line Privacy Litigation*,THE NEW YORK LAW JOURNAL (2000).
11. Samuel D Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193 (1890).
12. B.K.Mishra, *Indian Constitution is a living document: Expert,* The Times of India, (April 15, 2021).
13. Krishnadas Rajagopal, *The lowdown on the right to privacy*, The Hindu, (July 29, 2017).
14. Guido Noto La Diega, *The Internet of Citizens: A Lawyer's View on Some Technological Developments in the United Kingdom and India*, 12 Indian Journal of Law and Technology 53 (2016).
15. Bernard A. Berkman, *The Assault on Privacy: Computers, Data Banks, and Dossiers, by Arthur R. Miller*, 22 CASE W. RSRV. L. REV. 808 (1971).
16. Aditi Subramaniam &Sanuj Das, *In a nutshell: data protection, privacy and cybersecurity in India*, Lexology, (October 22, 2020).
17. Rachit Bahl, Aprajita Rana & Aman Gera, *Q&A on Data Protection and Cybersecurity*, (May 11th, 2020).
18. *IFF Releases Legislative Brief on Digital Rights for the Monsoon Session of the Parliament, Internet Freedom Foundation*, INTERNET FREEDOM FOUNDATION,(July 24th, 2021).
19. Namrata Maheshwari & Greg Nojeim, *Part 2: New Intermediary Rules in India Imperil Free Expression, Provacy and Security*, Center for Democracy & Technology, (June 04th, 2021).
20. Vrinda Bhandari & Renuka Sane, *Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018*, 14 Socio-Legal Review 143 (2018).
21. Varun Kalra, and Ramisha Jain, *An Armistice between Right to Privacy and Right of Surveillance*, 4 INDIAN JOURNAL OF LAW & PUBLIC POLICY 1-23 (2017).
22. Dhiraj Kukreja, *Securing Cyberspace*, 2 LIBERAL STUDIES 59-68, (2017).
23. Bhairav Acharya, *Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or*

Information) Rules, 2011, The Centre for Internet & Society, (31st March, 2013).

24. Vinod Basu, Protiti Base &Ashwarya Bhargava, *A Review of the Information Technology Rules, 2011 Reasonable Security Practice and Procedures and Sensitive Data or Info,* Mondaq, (MARCH 19, 2020).
25. *IFF files rejoinder in PIL seeking surveillance reform*, Internet Freedom Foundation, (23rd April, 2019).
26. Kritika Bhardwaj, *Preserving Consent within Data Protection in the Age of Big Data*, 5 NATIONAL LAW UNIVERSITY DELHI STUDENT LAW JOURNAL 100-110 (2018).
27. Namrata Maheshwari & Emma Llanso, *Part 1: New Intermediary Rules in India Imperil Free Expression, Privacy and Security*, Center for Democracy & Technology(May 25th, 2021).
28. Sidhartha and Pankaj Doval, *Rules protect rights of users, were framed because social media giants failed to do so: IT and law minister Ravi Shankar Prasad*, The Times of India,(June 01st, 2021).
29. Debopama Bhattacharya, *The Information Technology (IT) Rules, 2021*, MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES, (June 04th, 2021).
30. *Centre asks WhatsApp to withdraw 'discriminatory privacy policy, gives 7days to respond*, The Week,(May 19, 2021).
31. Kaushik Deka, *The battle for online privacy*, India Today, (June 11, 2021).
32. Nandana James, *WhatsApp's new privacy policy: Yet another reason why India needs data protection law*, Business Line,(January 10,2021).
33. Prasid Banerjee & Richa Banka, *WhatsApp case in Delhi HC first big test of privacy* LivMint (May 27th, 2021).
34. Neha Alawadhi, *Personal data protection bill JPC gets new chief in P P Chaudhary*, Business Standard,(July 22, 2021).
35. Anurag Vaishnav, *The Personal Data Protection Bill, 2019: All you need to know*, 2019, PRS Legislative Research,(December 23rd, 2010).
36. Rishab Bailey, *The issues around data localisation*, The Hindu, (February 25th, 2020).
37. Arun Prabhu, *The Personal Data Protection Bill 2019, An Analysis*, A Cyril AmarchandMangaldas Blog,(December 12th, 2019).

38. Probir Roy Chowdhury, YajasSetlur& Kavya Katherine Thayil, *Why data privacy must be safeguarded, even in times of COVID-19*, Financial Express, (May 19th, 2020).
39. Manya Gupta & Sunanda Tewari, *Tipping the Scale: Weighing Personal Data Protection Bill, 2019 against EU's GDPR*, First Post, (December 18th, 2019).
40. Pavan Duggal, *Cyber data privacy in peril*, The Tribune, (January 20th, 2021).
41. Purushotham Kittane, Inika Serah Charles, Aaron Kamath & Gowree Gokhale, *Privacy and Data Protection-India Wrap* 2020, The National Law Review, Volume XI Number 244, September 1st, 2021.
42. *Save our Privacy, A public brief and analysis on the Personal Data Protection Bill, 2019*, Internet Freedom Foundation.
43. Anil Sasi & Pranav Mukul, *WhatApp vs. Govt: The two cases in HC, each side contradicts itself*, The Indian Express, (June 07th, 2021)
44. *Whatsapp challenges intermediary Rules, says traceability will break end-to-end encryption, breach privacy; Union of India says no Fundamental Right is absolute*, SCC Online, (May 27th, 2021)
45. Joseph Menn, *WhatsApp sues Indian government over new privacy* rules, Reuters, (May 26th, 2021).