THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES

Kalamassery, Kochi – 683503, Kerala, India

DISSERTATION

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF LAW (LL.M.) DEGREE IN CONSTITUTIONAL AND ADMINISTRATIVE LAW (2024-2025) ON THE TOPIC

STATE SURVEILLANCE AND RIGHT TO PRIVACY IN INDIA

SUBMITTED BY

KRISHNENDU RAJ

(REGISTER NO-LM0124011)

UNDER THE GUIDANCE AND SUPERVISION OF

DR. ABHAYACHANDRAN.K

Associate Professor, Nuals, Kochi

CERTIFICATE

This is to certify that **Ms. KRISHNENDU RAJ**, Reg. No. - LM0124011, has submitted her dissertation titled **"STATE SURVEILLANCE AND RIGHT TO PRIVACY IN INDIA"** in partial fulfilment of the requirement for the award of Degree of Masters of Laws in Constitutional and Administrative Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that the dissertation submitted by her is original, bona fide and genuine.

DR. ABHAYACHANDRAN.K
GUIDE AND SUPERVISOR
NUALS, KOCHI

DATE: 28/05/2025
PLACE: ERNAKULAM

DECLARATION

I declare that this dissertation titled **"STATE SURVEILLANCE AND RIGHT TO PRIVACY IN INDIA"** is researched and submitted by me to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirement for the award of Degree of Master of Laws in Constitutional Law and Administrative Law, under the guidance and supervision of **Dr. Abhayachandran. K**, Associate Professor. It is an original, bona fide and legitimate work pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other University.

KRISHNENDU RAJ
REG NO-LM0124011
LLM (CAL)

DATE: 28/05/2025
PLACE: ERNAKULAM

ACKNOWLEDGEMENT

I extend my deepest gratitude to **Dr. Abhaychandran K, Associate Professor** for his invaluable guidance, insightful feedback, and unwavering support throughout the course of this dissertation on **"STATE SURVEILLANCE AND THE RIGHT TO PRIVACY."** His expertise and profound understanding of constitutional law have been instrumental in shaping my research, enabling me to critically examine the complex interplay between State surveillance and individual freedoms. His meticulous supervision and constructive criticism have significantly contributed to the intellectual rigor of this work.

I would like to covey my gratitude, **Hon'ble Mr. Justice S. Siri Jagan, Vice Chancellor**, NUALS, for his constant encouragement and support. I extend my sincere gratitude to **Dr. Anil R Nair, Associate Professor** and Chairperson, Centre for Post Graduate Legal Studies and Director, Centre for Parliamentary Studies and Law Reforms , NUALS, for his support and encouragement extended throughout the course.

I would like to further extend my deep felt gratitude to all the faculties of NUALS for their constant encouragement. I also convey my thankfulness to all non-teaching staffs of NUALS, for their timely assistance and also the technical team of NUALS for providing me with accurate technical aid and support.

Finally, I express my heartfelt gratitude to my parents, my brother, and my friends for their unwavering support, patience, and encouragement throughout this academic endeavour. Their belief in my capabilities has been a constant source of motivation.

Above all, I express my acknowledgments to the almighty for the blessings showered on me which lead to the successful and timely completion of this dissertation.

KRISHNENDU RAJ

PREFACE

As an LL.M. candidate specializing in Constitutional and Administrative Law at the National University of Advanced Legal Studies, my academic exploration has consistently gravitated toward questions at the intersection of technology, fundamental rights, and state accountability. Among the many compelling issues shaping contemporary legal discourse, the evolving tension between state surveillance and the right to privacy emerged as a particularly critical area of inquiry one that is both constitutionally profound and socially urgent.

The 2017 landmark decision in Justice K.S. Puttaswamy v. Union of India marked a constitutional watershed by affirming the right to privacy as intrinsic to the right to life under Article 21. Yet, despite this affirmation, India's parallel expansion of state surveillance through initiatives such as Aadhaar, the Central Monitoring System, and facial recognition technologies raises complex questions about the operational limits of privacy in a digital democracy. It is this paradox between constitutional guarantees and practical governance that catalysed the central research focus of this dissertation.

This study critically engages with the legal, institutional, and philosophical underpinnings of privacy in the face of increasing executive power exercised through technological surveillance. It probes whether India’s current statutory frameworks, including the Information Technology Act, the Telecommunication Act, and the Digital Personal Data Protection Act, adequately safeguard individual autonomy in light of global human rights standards. The dissertation further interrogates the compatibility of surveillance practices with democratic values and constitutional morality, drawing from both Indian jurisprudence and comparative international perspectives.

By tracing judicial interpretations, legislative lacunae, and the normative foundations of privacy, this research seeks to contribute to a deeper understanding of how legal systems can reconcile national security imperatives with the protection of fundamental rights. Ultimately, this work endeavours to present a rights based framework for surveillance regulation that upholds accountability, transparency, and democratic oversight principles essential to preserving the dignity and liberty of every citizen.

ABBREVIATIONS

AFRS	Automated Facial Recognition System
BEAP	Brain Electrical Activation Profile
CAIR	Centre for Artificial Intelligence and Robotics
CBDT	Central Board of Direct Taxes
CBI	Central Bureau of Investigation
CCTNS	Crime and Criminal Tracking Network System
CCTV	Closed-Circuit Television
C-DOT	Centre for Development of Telematics
CMS	Central Monitoring System
CNIL	National Commission on Informatics and Liberty
CRC	Convention on the Rights of the Child
DPA	Data Protection Authority
DPDP	Digital Personal Data Protection Act
DPI	Deep Packet Inspection
DRDO	Defence Research and Development Organisation
DYBBS	Digi Yatra Biometric Boarding System
ED	Enforcement Directorate
EU	European Union
FRT	Facial Recognition Technology
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IB	Intelligence Bureau
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICCPR	International Covenant on Civil and Political Rights
IPOA	Indian Post Office Act, 1898

ISF	Interception Store & Forward
IT	Information Technology Act (2000)
ITA	Indian Telegraph Act, 1885
MCOCA	Maharashtra Control of Organized Crime Act
NATGRID	National Intelligence Grid
NETRA	Network Traffic Analysis
NIA	National Investigation Agency
NSA	National Security Agency
OHCHR	Office of the High Commissioner for Human Rights
PUCL	People's Union for Civil Liberties
R&AW	Research and Analysis Wing
RMC	Regional Monitoring Centre
TSP	Telecom Service Provider
UDHR	Universal Declaration of Human Rights
UNCITRAL	United Nations Commission on International Trade Law
UNCRC	United Nations Convention on the Rights of the Child
UNO	United Nations Organization
UOI	Union of India
UPA	United Progressive Alliance
US	United States

TABLE OF CASES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Background

In India, the right to privacy is constitutionally recognised as an essential component of the right to life and personal liberty under Article 21. The landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India[1] affirmed that privacy is not merely a peripheral right, but one that is central to personal autonomy, human dignity, and democratic citizenship. This recognition becomes especially significant in the face of increasing state led surveillance, which, under the guise of security and administrative necessity, often encroaches upon individual freedoms without adequate legal safeguards or oversight.

The philosophical roots of privacy as a legal right can be traced back to the seminal work of Warren and Brandeis, who conceptualised it as "the right to be let alone."[2] Brandeis warned that modern technological advancements could inflict mental and emotional injury far greater than physical harm, and privacy was essential for preserving the sanctity of human personality. This early vision continues to resonate in the digital age, where the contours of surveillance have expanded from physical observation to invisible, data driven monitoring.

In today's technologically mediated environment, surveillance has become deeply embedded in the structure of everyday life. Government agencies increasingly collect, store, and analyse large volumes of personal data ranging from communication records and location history to social media activity. These forms of surveillance are not always overt, and in many cases, individuals are unaware that they are being monitored. The

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1
[2] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, (1890).

lack of transparency surrounding these operations significantly reduces the ability of citizens to challenge or question how their personal information is used.

This asymmetry of power between the state and the citizen lies at the heart of the constitutional dilemma. While the state claims that surveillance is necessary to combat crime, maintain public order, or safeguard national security, the absence of statutory regulation, judicial oversight, and independent accountability mechanisms makes such powers vulnerable to abuse. Surveillance, when left unchecked, cultivate a culture of fear and self-censorship. It can inhibit freedom of expression, suppress dissent, and undermine the very foundations of democratic participation.[3] Moreover, the digital permanence of data collected during surveillance intensifies the threat to privacy. Every click, message, or interaction leaves a trace that can be analysed, profiled, and stored indefinitely. The citizen is transformed from a rights bearing subject into a data point within a vast bureaucratic infrastructure. This shift risks normalising intrusive governance and expanding the state's reach into intimate aspects of life often without necessity, proportionality, or accountability.

1.2 Research Problem

In the absence of a comprehensive legal framework regulating surveillance practices, the balance between state power and individual liberty remains dangerously tilted. Current mechanisms are fragmented and often operate through executive discretion, lacking the procedural safeguards necessary to protect fundamental rights. The need for a rights based approach to surveillance, guided by constitutional principles and subject to democratic controls, is urgent and undeniable.

At its core, the right to privacy serves as a bulwark against arbitrary state intrusion. It enables individuals to think, speak, associate, and live freely shielded from the fear of constant monitoring. As India continues to adopt and implement data centric governance models, protecting the individual's privacy must not be viewed as a secondary concern, but as an essential element of constitutional democracy. The tension between surveillance and privacy thus represents not merely a technological issue, but a constitutional crisis one that demands immediate legal, institutional, and ethical

[3] Gautam Bhatia, State Surveillance and the Right to Privacy in India: A Constitutional Perspective, 26(1) Nat'l L. Sch. India Rev. 127, 139–40 (2014).

responses. This research seeks to critically examine whether India's existing legal framework on state surveillance effectively balances the requirements of protection of individual privacy rights, while also ensuring compliance with constitutional principles and international standards.

1.3 Statement of Problem

- The rapid expansion of state surveillance in India, driven by advancements in technologies such as biometrics, artificial intelligence, and facial recognition systems, has intensified concerns about data protection and privacy.
- This raises critical questions about effectiveness of privacy safeguards in the country. Specifically, there is a need to examine whether the Right to Privacy, as recognized by the Indian Constitution, can be upheld as an absolute right in the context of mass surveillance.
- Additionally, the adequacy of existing legal frameworks, including the Information Technology Act 2000, Indian Telecommunication Act, 2023 and the Digital Personal Protection Act 2023, must be assessed to determine their effectiveness in protecting individual privacy against evolving surveillance challenges.
- Furthermore, it is imperative to analyze the extent to which India’s surveillance practices and legislation align with international standards, ensuring compliance with global norms while safeguarding constitutional principles**.**

1.4 Scope and relevance of study

The study provides a comprehensive analysis of state surveillance practices in India and their implications for constitutionally protected privacy rights. By focusing on legislative frameworks, it critically evaluates how these laws address the challenges posed by advanced surveillance technologies

1.5 Objectives

1. To analyse the concept of privacy as a fundamental right in India and its limitations within the context of state surveillance.
2. To assess the effectiveness of current legal frameworks, such as the Information Technology Act and the Telegraph Act, in protecting privacy.
3. To evaluate India's compliance with international standards on privacy and surveillance, identifying gaps and potential reforms in legal protections against state surveillance.

1.6 Hypothesis

India's current laws and regulations on state surveillance inadequately balance the state surveillance needs with individual privacy rights, which could lead to violations of constitutional privacy protections.

1.7 Research Questions

1. Whether Right to Privacy is an absolute right?
2. Are existing Indian laws, such as the Information Technology Act, adequate to protect individual privacy in the age of mass surveillance?
3. To what extent has India aligned its surveillance practices and laws with international rules on surveillance?

1.8 Methodology

The methodology adopted in this dissertation is a doctrinal legal research approach

1.9 Limitation of Research

The study is limited by the availability of empirical data on state surveillance practices

1.10 Literature Review

1. **Swaminathan & Basu, *Surveillance and Data Protection: Threats to Privacy and Digital Security* (2020):** This report examines the pervasive expansion of state surveillance in India through technologies like facial recognition systems, Pegasus spyware, and contact-tracing apps. The authors argue that these tools, often deployed without adequate legal safeguards, erode civil liberties, chill dissent, and undermine democratic participation. Legal instruments such as the Indian Telegraph Act and IT Act are critiqued for lacking robust oversight and transparency. The report further explores controversial proposals like Aadhaar-social media linkage and traceability mandates on encrypted platforms. Ultimately, the authors advocate for surveillance reform grounded in legality, necessity, and proportionality, aligning with international human rights norms.

2. **Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography* (2014)**: Bhatia traces the constitutional evolution of the right to privacy in India through judicial decisions from M.P. Sharma and Kharak Singh to Gobind and Puttaswamy. He critiques India's surveillance regimes like CMS and Netra for operating without sufficient statutory backing, and highlights the judiciary's gradual recognition of privacy under Article 21. Drawing from American Fourth Amendment jurisprudence, Bhatia situates privacy within the broader framework of dignity, autonomy, and liberty. His analysis of the "chilling effect" of state surveillance on individual freedoms emphasizes the need for legislative accountability. The article serves as a critical legal narrative of how Indian constitutional law has responded often inconsistently to growing surveillance powers.

3. **Jan Holvast, *History of Privacy*, in *The Future of Identity* (2009)**: Holvast presents a historical overview of privacy, from ancient concepts of solitude to

modern concerns about informational autonomy. He links privacy's development to technological advances, especially the rise of computers and data collection systems. The chapter explores the dual nature of technology offering both tools for privacy protection and mechanisms of surveillance. Holvast highlights the foundational works of Warren & Brandeis and Alan Westin, stressing privacy as essential for personal autonomy, emotional release, decision-making, and protected communication. Post-9/11 shifts in global policy, he argues, have favored state surveillance over privacy protections. He concludes that without renewed political will, societies risk normalizing a surveillance culture that compromises both freedom and democracy.

4. **Tejas Jindal, *Right to Privacy as a Fundamental Right in India: Evolution, Challenges and the Impact of Digitalization* (2024)**: Jindal's article traces the constitutional development of privacy in India, culminating in the *Puttaswamy* (2017) judgment. He contextualizes privacy as intrinsic to individual dignity and liberty and explores how emerging digital technologies like facial recognition and surveillance systems challenge traditional privacy frameworks. The article critiques the lack of legislative safeguards and underscores the urgency of enacting comprehensive data protection laws. Drawing comparisons with global standards such as the GDPR, Jindal emphasizes the need for a balanced model that safeguards privacy without stifling innovation.

5. **Adrienn Lukács, *What is Privacy? The History and Definition of Privacy* (2020)**: Lukács offers a conceptual and historical exploration of privacy, arguing that its definition varies by era, culture, and context. She organizes privacy into six conceptual categories secrecy, intimacy, personhood, control over information, autonomy, and limited access and critiques attempts to provide a single, exhaustive definition. Drawing on theorists like Westin, Fried, and Solove, she proposes that privacy must be interpreted contextually. Lukács supports a pluralist model, combining definitional clarity with adaptability to emerging technologies and evolving societal expectations.

6. **Tathagata Satpathy, Karnika Seth & Anita Gurumurthy, *Are India's Laws on Surveillance a Threat to Privacy?* (2018)**: This article critiques India's expanding surveillance framework post Puttaswamy, particularly under Section 69 of the IT Act, 2000. The authors argue that executive orders allowing multiple state agencies to intercept digital communications lack transparency, oversight, and proportionality. They express concern that such practices signal a shift toward a surveillance state, where privacy is routinely compromised in the name of internal security. While acknowledging the importance of surveillance in national security, the article calls for legislative checks to ensure that privacy remains protected within constitutional bounds.

7. **Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087 (2002)**: Solove challenges the traditional essentialist approaches to privacy, which often fail to capture its multifaceted nature. Drawing from Wittgenstein's theory of "family resemblances," he argues that privacy should be understood not as a fixed category but through its practical manifestations in various social and legal contexts. He identifies six major conceptions of privacy ranging from intimacy and secrecy to personhood and informational control and advocates a pragmatic approach that focuses on the harms privacy violations cause. His work offers a flexible framework for addressing privacy concerns in an era of rapid technological change

8. **Kush Kalra, *Right to Privacy Under Indian Constitution*, GIBS Law Journal (2020)**: Kalra's article provides a doctrinal exploration of the constitutional basis of the right to privacy in India. Tracing its evolution from early common law to contemporary Article 21 interpretations, the piece examines how privacy has transitioned from a moral notion to a justiciable right. The article analyzes key cases such as Kharak Singh, Gobind, and Rajagopal, emphasizing the Supreme Court's role in incorporating privacy within the ambit of personal liberty. Kalra also evaluates permissible restrictions on privacy through legislative, administrative, and judicial actions. By referencing both Indian and international jurisprudence, the article offers a comprehensive understanding of privacy as a multidimensional concept involving autonomy, secrecy, and control over personal information.

9. **Arghish Akolkar, *Government Surveillance Against the Right to Privacy in Cyberspace in India*, EJSSS (2024)**: Akolkar's work critiques India's growing digital surveillance apparatus within the context of constitutional privacy protections. He traces the legislative lineage from colonial laws like the Indian Telegraph Act to the contemporary IT Act and the Digital Personal Data Protection Act, 2023. The article highlights how opaque agreements between the state and service providers facilitate mass and targeted surveillance. It raises alarms about vague terms like "public emergency" and the lack of independent oversight, especially concerning Pegasus and metadata collection. Arguing that digital surveillance risks normalizing suspicion and executive overreach, Akolkar calls for greater judicial scrutiny and legal safeguards to protect individual liberties in cyberspace.

10. **Buddhadeb Halder, *Privacy in India in the Age of Big Data*, Digital Empowerment Foundation (2020)**: Halder's report delves into how big data technologies threaten privacy in India, especially amid public-private data-sharing arrangements. He explores how government programs like Aadhaar, Smart Cities, and MGNREGA collect and process vast datasets, often lacking robust access controls and transparency. The study contextualizes privacy within international legal norms, referencing instruments like the UDHR and ICCPR. Halder critiques the surveillance potential of metadata and the Internet of Things, emphasizing how poorly regulated data ecosystems jeopardize rights. His work concludes with a call for implementing the UN Special Rapporteur's Ten-Point Action Plan to establish a human rights–centric data protection framework in India.

11. **Chaitanya Ramachandran, *PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for the Digital Age*, NUJS Law Review (2014)**: Ramachandran critically re-examines the *PUCL v. Union of India* judgment, which laid foundational safeguards against telephone tapping. He argues that while the 1996 PUCL guidelines were pivotal in curbing surveillance abuse, they are insufficient in the era of mass digital surveillance. Citing the rise of systems like CMS and Netra, the article advocates for comprehensive surveillance law reform. Ramachandran underscores how existing legal frameworks have failed to adapt to Internet-based communication, risking arbitrary state action. He concludes

that the PUCL framework must be reimagined to include transparency, oversight, and proportionality principles to safeguard privacy in the digital era.

12. **Poonam Rawat & Shreyes Aggarwal, *Right to Privacy and Data Protection: Issues in India*, IJCRT (2020)**: This article investigates the intersection of privacy and data protection in India's evolving legal and technological context. The authors argue that despite Article 21's expansive interpretation, existing data protection frameworks, including the IT Act, are inadequate. They trace privacy's philosophical origins from ancient Indian texts to modern jurisprudence, highlighting its connection to autonomy and dignity. The article stresses the inadequacy of current legislation in addressing the threats posed by mass data collection, particularly in welfare schemes. It advocates for distinct and robust data protection laws aligned with international standards to effectively balance state interests with citizens' informational privacy.

13. **Naseem Ahmed & Faiz Khan, *The Erosion of Privacy in the Face of State Surveillance: A Digital Dystopia* (2024)**: Ahmed and Khan critically examine the growing threat posed by state surveillance to individual privacy in India. The article traces constitutional developments, emphasizing how Article 21, though judicially interpreted to include privacy, faces strain under intrusive technologies. The authors highlight structural issues in Indian legal systems that enable overreach, referencing surveillance tools and policy initiatives like Aadhaar. Drawing parallels with global human rights discourse, they argue that unchecked surveillance diminishes human dignity and autonomy. The paper calls for urgent legislative reform and privacy-conscious governance to prevent India from becoming a digital surveillance state.

14. **Alibeigi, A.B. Munir & M.D. Ershadul Karim, *Right to Privacy: A Complicated Concept to Review* (2019)**: This article explores the multidimensional nature of privacy through a comparative legal lens. The authors argue that privacy, despite being a fundamental human desire, defies uniform definition due to cultural, legal, and technological diversity. Drawing on sociology, law, and philosophy, they distinguish between physical, informational, and decisional privacy. They also highlight the evolution of privacy through U.S. tort law and European human rights

jurisprudence. Emphasizing contextual variability, the authors call for a rights-based, adaptive understanding of privacy aligned with international norms and emerging digital risks.

15. **Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy* (1890)**: This landmark article introduced the modern legal concept of privacy as "the right to be let alone." Warren and Brandeis argue that common law must evolve to protect emotional and spiritual integrity alongside physical and proprietary rights. Motivated by media intrusion and photographic technology, they advocate for tort-based remedies to unauthorized publication and personal invasions. Their article laid the foundation for informational and decisional privacy doctrines and remains influential in American and global privacy jurisprudence, especially in justifying constitutional recognition of non-enumerated rights in digital contexts.

16. **Addison Litton, *The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression* (2015)**: Litton's article critically examines India's Central Monitoring System (CMS) as a potent surveillance tool with serious consequences for privacy and democratic free speech. Drawing comparisons with the U.S. NSA's PRISM program, the study shows that CMS allows nine government agencies to access telecommunications and internet data without judicial oversight or parliamentary scrutiny. Litton highlights that CMS promotes a climate of self-censorship, replacing prior models of intermediary-based content regulation with direct state intrusion. The article critiques vague provisions under the IT Act (Sections 69, 69A, and 66A) for enabling arbitrary censorship. The analysis concludes that CMS weakens public discourse and civil liberties by fostering opacity, bypassing procedural safeguards, and undermining accountability in India's surveillance infrastructure.

17. **Sargam Thapa, *The Evolution of Right to Privacy in India*, (2021)**: Thapa offers a thorough historical and jurisprudential account of the evolution of the right to privacy in India. Beginning with ancient texts such as the *Dharmashastras*, *Hitopadesha*, and *Arthashastra*, the article argues that privacy was deeply embedded in Indian philosophical thought. Moving to colonial-era frameworks and

the Constituent Assembly debates, Thapa explains how right to privacy was initially excluded from the constitutional text. The article then tracks judicial developments from M.P. Sharma and Kharak Singh to Puttaswamy (2017), where the Supreme Court finally declared privacy a fundamental right under Article 21. Thapa emphasizes how constitutional recognition, global norms, and technological pressures have collectively reshaped privacy as a central democratic concern in India

1.11 Chapterisation

Chapter 1: Introduction
This chapter deals with the introduction of this paper, research design, objectives and methodology.

Chapter 2: The Right to Privacy: A Theoretical Perspective
This chapter examines the theoretical foundations, historical evolution, and global recognition of the right to privacy.

Chapter 3: Judicial Oversight and the Right to Privacy in India
This chapter critically examines the role of the Indian judiciary in recognizing, shaping, and safeguarding the right to privacy, with particular emphasis on landmark rulings, constitutional interpretation under Article 21, and the evolving judicial standards of proportionality and oversight in surveillance matters.

Chapter 4: State Surveillance: An Overview
This chapter deals with the evolution of surveillance practices in India, from colonial-era intelligence controls to present-day digital systems like CMS, NATGRID, and Aadhaar. It examines the nature of mass and targeted surveillance and critically evaluates state justifications in light of constitutional privacy protections.

Chapter 5: Legal Frameworks and Regulatory Gaps: An Analytical Overview
This chapter deals with the statutory basis of surveillance in India, analysing laws such as the IT Act, DPDP Act, Telecom Act, and Aadhaar Act. It highlights key legal gaps

including lack of judicial oversight, vague standards, and executive overreach, arguing that these undermine the privacy safeguards.

Chapter 6: Conclusion and Suggestions

The final chapter presents the key findings of the study and outlines suggestions aimed at strengthening and operationalizing a surveillance framework in India.

CHAPTER 2

THE RIGHT TO PRIVACY: A THEORETICAL PERSPECTIVE

2.1 Introduction

The birth of the Right to Privacy was as old as mankind. The inception of Privacy as an idea in the law can be traced back to the well-known article published in the Harvard Law Review in 1890 by Samuel Warren and Louis Brandeis, named "The Right to Privacy."[4] They originally described the right to Privacy as an existing common law right, which included protections against invasions of every person's inviolable personality. According to them, Privacy is defined as a right to be let alone and a right of each individual to determine, under ordinary circumstances, what their thoughts, sentiments, and emotions should be when communicating with others[5]. In Privacy and Freedom, Alan Westin defines Privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, Privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve"[6]. Privacy is a state of psychological security, a condition in which a person can stand before others and have their personality reflected in their souls as they see fit.[7]

Privacy holds a fundamental position in domestic and international legal frameworks. Privacy is enshrined in various international human rights instruments, underlining its

[4] Samuel D. Warren ,Supra note 2
[5] Jan Holvast, History of Privacy, in The Future of Identity 13, 13–42 (V. Matyas et al. eds., IFIP AICT 298, 2009).
[6] Id., Pg. 16
[7] Dorothy J. Glancy, The Invention of the Right to Privacy, 21 ARIZ. L. REV. 1 (1979).

universal significance. Despite its global recognition, Privacy lacks a universally accepted definition. Several jurists have tried to define Privacy, but due to the vast changes in the sphere of Privacy relating to individuals, most of this definition only points out any single aspect.

2.2 Evolution

The Concept of Privacy in the ancient world was not as quietly acknowledged as it is today. Even though the idea of Privacy existed in ancient Greece, it was not a foundational tenet of society. Daniel L. Solove notes that the division of society by Aristotle into Polis and Oikos, the public sphere, or the polis, was perceived as a realm of importance; in contrast, the private sphere, or the Oikos (home and family), was considered secondary. The private realm was primarily valued for enabling individuals to participate in the public realm, regarded as the accurate measure of human existence. In this sense, Privacy was regarded as a prerequisite for active civic life but not an unalienable right. Similarly, the Romans emphasized the public sphere as a venue where an individual potential could be realized, placing a higher value on social interactions[8].

Privacy evolved from a secondary aspect of public life to a crucial aspect of individuality. According to Rousseau, Privacy is a separation from social norms in the home and society. Hannah Arendt argued that Privacy is essential for personal identification and exercising political rights, even though we understand our reality and the shared world around us through connections with others[9].

In the Medieval Age, there was no such thing as Privacy as what exists in today's sense. Instead, the individual lived as an integral member of a community. As such, their private life was adversely affected by the ongoing monitoring conducted by other members of the society. In Shakespeare's time, Privacy had unfavourable views, reflecting societal concerns about its potential for disruption. In plays like “Love's Labour's Lost” and “The Tempest”, solitude and private contemplation are associated

[8] Keigo Komamura, Privacy’s Past: The Ancient Concept and Its Implications for the Current Law of Privacy, 96 WASH. U. L. REV. 1337 (2019).
[9] Id.

with suspicion, vice, and political conspiracy. Characters who recede into Privacy often act deceitfully or subversively, harming social and political order[10].

This perspective aligns with the Renaissance emphasis on communal life and the natural hierarchy, where kings are governed by divine right. Privacy was viewed not as a space for self-expression but as an indicator of instability and a threat to societal harmony.[11] However, while the dominant societal model of the Renaissance emphasized communal life and natural hierarchy, an intellectual shift was simultaneously underway. Enlightenment thinkers such as John Locke began to articulate a counterpoint that prioritized personal liberty and individual autonomy. His emphasis on the sanctity of individual rights subtly reaffirmed privacy as a necessary element of freedom. Locke laid a philosophical foundation for the modern understanding of privacy as integral to human dignity and self-determination by arguing that individuals are entitled to control over their person and property. According to Locke, setting up a government and making laws was only a secondary transaction between individuals, the primary being preserving life, liberty, and property. According to him, people give up only a part of their natural rights while abandoning the 'state of nature,' the remaining natural rights like life, liberty, and property are kept intact. [12]

2.2.1 Industrialization and Privacy Concerns

Rapid industrialization and urbanization changed the economy and culture over the 19th century, precipitating profound transformations in societal structures, economic systems, and interpersonal relationships. The mass migration of individuals to urban centres in pursuit of employment opportunities led to the emergence of densely populated cities, where people were compelled to live in close quarters with unfamiliar others[13]. This physical proximity and the advent of industrial labour systems and rigidly structured schedules diminished the scope for personal and familial autonomy that had been more readily accessible in rural agrarian societies. Consequently,

[10] Id.
[11] John Locke, Two Treatises of Government (Peter Laslett ed., Cambridge Univ. Press 1988)
[12] Sjoerd Keulen & Ronald Kroeze, Privacy from a Historical Perspective, in The Handbook of Privacy Studies 15 (Bart van der Sloot & Aviva de Groot eds., Amsterdam Univ. Press 2018).
[13] Adrienn Lukács, What Is Privacy? The History and Definition of Privacy (Ph.D. thesis, Univ. of Miskolc, 2016)

individuals increasingly prioritized safeguarding their personal and domestic lives from the pervasive scrutiny of neighbours, employers, and the broader public. Ironically, although urban life offered some degree of anonymity, it also heightened the longing for private spaces where people could build personal identities distinct from their public portrayals.

Another significant change was the emergence and expansion of (tabloid) newspapers, which provided a thriving environment for gossip and photojournalism. By the 19th century, as journalism became increasingly popular, there was a growing tendency to exploit individuals' privacy for financial gain, prompting greater concern over the need to control personal data. The telegraph revolutionized communication but simultaneously exposed private correspondence to the risk of interception and unauthorized access. Samuel D. Warren and Louis D. Brandeis were the first to identify the privacy risks posed by societal and technological advancements. Following the publication of the article The Right to Privacy, in 1890, the concept of privacy became the focus of numerous works. These publications primarily describe the idea of privacy and the developments of techniques invading privacy, especially computers, which are seen as the primary source of privacy invasion.[14]

2.2.2 Judicial Recognition in the United States

Privacy rights gained further momentum in the mid-20th century through a series of landmark U.S. Supreme Court decisions that arose in response to increasingly invasive state actions. In Olmstead v. United States (1928)[15], the majority ruled that warrantless wiretapping of a suspect's phone lines did not violate the Fourth Amendment since it involved no physical trespass. This interpretation effectively permitted covert state surveillance without judicial oversight, thereby enabling privacy violations under the guise of procedural technicalities. However, in dissent, Justice Louis Brandeis upheld the right to privacy in every individual and coined the classic and crisp definition of privacy as the right to be let alone. He asserted that the purpose of privacy was to secure conditions favourable to the pursuit of happiness, protecting the spiritual nature of man

[14] Id.
[15] Olmstead v. United States, 277 U.S. 438 (1928)

his feelings and his intellect from unjustified government intrusion. Brandeis warned that evolving technologies posed unprecedented threats to liberty and that privacy must be protected even in the absence of physical invasion.

The U.S. Supreme Court recognized more direct state interference in the private sphere in Griswold v. Connecticut (1965)[16], where a state law prohibiting the use of contraceptives by married couples was struck down. The Court found that the law violated the sanctity of marital privacy, holding that various provisions of the Bill of Rights created penumbras of privacy into which the state could not intrude. The decision marked an important constitutional acknowledgment that intimate family decisions were beyond the legitimate reach of the government.

The understanding of privacy was further expanded in Katz v. United States (1967)[17], which dealt with government eavesdropping on a public telephone booth. The Court ruled that even in public spaces, individuals are protected if they have a reasonable expectation of privacy. This decision rejected the outdated trespass doctrine from Olmstead[18] and recognized that electronic surveillance could constitute a serious invasion of personal liberty. Justice Harlan's concurrence introduced a two-prong test that continues to guide privacy analysis: first, whether the individual had an actual expectation of privacy, and second, whether that expectation is one that society is prepared to recognize as reasonable.

This jurisprudence evolved further in Eisenstadt v. Baird (1972)[19], where the Court invalidated a law that prohibited unmarried individuals from accessing contraceptives. The ruling was significant because it extended privacy rights beyond the marital relationship, affirming that the right to make intimate decisions was inherent in individual autonomy, regardless of marital status. The Court held that treating unmarried persons differently violated both the Equal Protection Clause and the substantive right to privacy, thus correcting a discriminatory state practice.

[16] Griswold v. Connecticut, 381 U.S. 479 (1965).
[17] Katz v. United States, 389 U.S. 347 (1967).
[18] Olmstead v. United States, 277 U.S. 438 (1928)
[19] Eisenstadt v. Baird, 405 U.S. 438 (1972).

The right to privacy was thereafter solidified and extended in a broader reproductive context through Roe v. Wade (1973)[20], in which a pregnant single woman challenged Texas laws criminalizing abortion except to save the mother's life. The Court held that these laws constituted a direct violation of a woman's right to privacy, protected under the Due Process Clause of the Fourteenth Amendment. It ruled that the right to terminate a pregnancy was part of the broader constitutional protection of personal autonomy and bodily integrity.

2.3 Global Recognition

In reaction to the horrific acts of World War 2, there was global recognition of privacy as a fundamental human right. The Universal Declaration of Human Rights (UDHR)[21], adopted by the United Nations in 1948, had given prominence to privacy at the international level. Even though it was the first document to deal with the Right to privacy, since it was in the form of a resolution of the General Assembly, it was not legally binding. Article 12 of the UDHR defines the Right to privacy as:

> *"No-one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law or against such interference or attacks."*

The UDHR marked the beginning of a normative shift, recognizing that privacy is essential not merely as protection from surveillance, but also as a precondition for the free exercise of thought, belief, expression, and personal development[22]. Its global influence has persisted through the International Bill of Human Rights, which integrates the UDHR with the International Covenant on Civil and Political Rights (ICCPR)[23] and the International Covenant on Economic, Social and Cultural Rights (ICESCR)[24].

[20] Roe v. Wade, 410 U.S. 113 (1973).
[21] G.A. Res. 217A (III), Universal Declaration of Human Rights (Dec. 10, 1948)
[22] Payal Thaorey**,** Legal Introspection Towards the Development of Right to Privacy as Fundamental Right in India, 11 INDONESIA L. REV. 3, art. 5 (Dec. 31, 2021).
[23] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
[24] International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S.3

The ICCPR was adopted in 1966 and came in force in 1976. It translated the aspirational values of the UDHR into binding legal commitments for its signatories.

According to Article 17 of ICCPR,

> *"No one shall be subjected to arbitrary or unlawful interference with his privacy family home and correspondence not to unlawful attacks on his honour and reputation".*

ICCPR emphasizes the protection of the Right to privacy for citizens in each country. It states that these fundamental rights derive from the inherent dignity of human beings[25].

Article 8 of the European Convention of Human Rights[26] set out the "Right to respect for private and family life:

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The United Nations International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families[27] also recognized the Right of privacy for migrant workers and their families. Article 14 of this Convention again followed Article 12 of the UDHR to protect migrant workers' privacy right. Article 14 specifies

[25] A. Alibeigi et al. Right to Privacy: A Complicated Concept to Review, 5 J. POL. & L. 1 (2019)
[26] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.
[27] International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Dec. 18, 1990, 2220 U.N.T.S. 3.

that migrant workers and their families have to be protected against any intrusion into their privacy, family, communication, and honour.

> *"No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks"*

The United Nations Convention on the Rights of the Child (UNCRC or CRC)[28] of 1989, followed UDHR under Article 16.

> *1. "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks."*

The Convention on the Rights of Persons with Disabilities[29], under Article 22, has recognized the privacy right for individuals with specific conditions.

> *1. "No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.*
>
> *2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others"*

[28] Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.
[29] Convention on the Rights of Persons with Disabilities, Dec. 13, 2006, 2515 U.N.T.S. 3.

This Convection is the newest human rights treaty which was adopted in 2006 by the United Nations General Assembly and entered into force on 3 May 2008[30].

2.4 Technological Advancements

By the mid-20th century, rapid technological advancements and the growing ability of governments and organizations to collect and analyse vast amounts of personal data brought privacy concerns to the forefront of public discourse. The advent of digitalization, particularly through the development of electronic databases, raised alarm over potential misuse, unauthorized access, and mass privacy violations. These innovations expanded the scope and scale of data collection, raising critical questions about personal liberty and informational autonomy[31].

The widespread adoption of computers further transformed data processing and storage, enabling institutions to compile large volumes of sensitive personal information. By the late 1970s, advances in telecommunications and integrated computing significantly heightened the risks especially the potential for unauthorized sharing of private data with unknown third parties[32].

In response to these escalating threats, governments around the world began enacting legal frameworks to safeguard personal data. This growing legislative movement sought to address the normalization of privacy intrusions in data-driven systems by laying down foundational principles of data governance, individual consent, and informational rights.

2.5 Legal Frameworks and Global Data Protection

Legal frameworks of many nations began to address the growing concerns surrounding data privacy. With Germany's ground breaking Hessen Data Protection Act (1970), the first law to control the use of personal data, data protection regulations began to take shape. The first national data privacy regulation, the Swedish Data Act (1973), came

[30] Payal Thaorey ,Supra Note 22
[31] Murni Wan Mohd Nor & Ratnawati Mohd Asraf, Technology and the Deterioration of Right to Privacy, 7 INT'L J. ASIA PAC. STUD. 37 (July 2011).
[32] Keigo Komamura ,Supra Note 9

next, creating the Data Inspection Board to monitor adherence. In the United States, the Privacy Act (1974) restricted federal agencies' use of personal data and granted individuals rights to access and amend their records. West Germany extended its protections nationally with the Federal Data Protection Act (1977)**,** while Denmark, Austria, France, Norway, and Luxembourg followed in 1978 with their comprehensive privacy laws, including the creation of enforcement bodies like France's National Commission on Informatics and Liberty (CNIL)**.** By the early 1980s, Western Europe saw widespread adoption of data protection frameworks, with nations like the Netherlands and Spain joining. This movement soon became global, with countries like Israel, Japan, and Canada introducing privacy laws in the 1980s, followed by 22 more nations worldwide in the 1990s. These legislations collectively established foundational principles for safeguarding personal information in an increasingly interconnected world.[33]

However, as many legal systems progressed toward safeguarding individual privacy rights, a parallel and often conflicting trend began to emerge. States increasingly employed mass surveillance technologies to serve their intelligence and control objectives. Consequently, the privacy discourse entered a more contentious phase, wherein assertions of national security frequently came into conflict with the protection of individual rights[34].

2.6 State Surveillance and the National Security Justification

As the Cold War intensified global tensions worldwide, Governments invested significantly in intelligence gathering technology to keep an eye on potential threats. These surveillance programs, however, often went beyond national security goals, raising worries about invasions of civilians' privacy[35]. The possibility of unrestricted government power brought into sparked discussion concerning about power abuse and the necessity to safeguard individual rights. The relationship between technology and

[33] Data Security Council of India**,** Legal Framework for Data Protection and Security and Privacy Norms (April 10,2025),https://www.dsci.in/files/content/knowledgecentre/2023/Legal%20Framework%20for%20Data%20Protection%20and%20Security%20and%20Privacy%20norms.pdf.
[34] Neil M. Richards, The Dangers of Surveillance, 126 HARV. L. REV. 1934 (2013).
[35] David Lyon, Surveillance Studies: An Overview (Polity Press 2007).

privacy underwent a significant transformation in the 20th century with the rapid development of surveillance systems, telecommunications, and computing. Tools such as eavesdropping devices, CCTV systems, and wiretaps enabled governments and organizations to monitor individuals with greater precision, fundamentally reshaping the concept of personal space. While technologies like the telephone revolutionized communication, they also introduced vulnerabilities particularly concerning the interception of private conversations[36].

These developments evolved into widespread communications surveillance, wherein both state and non-state actors employ big data analytics to monitor and analyse individuals' activities. This includes the collection, interception, retention, and use of information arising from a person's past, present, or even anticipated communications. As surveillance capabilities expanded, so too did public concern over unchecked state power and the gradual erosion of privacy[37].

This concern reached a critical point in the early 21st century, particularly after the September 11, 2001 attacks, which reshaped global security priorities. Invoking the need to combat terrorism, governments across the world enacted sweeping surveillance measures that institutionalized practices once limited to intelligence operations[38]. Consequently, the balance between civil liberties and national security shifted markedly, often to the detriment of individual privacy rights.

2.7The Post-9/11 Surveillance Regime

The idea of privacy is now multifaceted, covering a range of elements that go beyond the conventional idea of maintaining the confidentiality of personal data. Concerns about privacy have expanded in the digital era to include freedom from invasive surveillance technology as well as data protection. Under the guise of counterterrorism and national security initiatives, governments all over the world implemented vast and far-reaching surveillance operations in the wake of the September 11, 2001 attacks,

[36] Id.
[37] Murni Wan Mohd , Supra Note 31
[38] Clayton Northouse ed., Protecting What Matters: Technology, Security, and Liberty Since 9/11 (Brookings Inst. Press 2006).

frequently at the price of civil liberties and individual privacy[39]. The introduction of sweeping legislative frameworks, such as the USA PATRIOT Act[40] in the United States, greatly increased the authority of intelligence organizations by permitting indiscriminate electronic communications monitoring, warrantless wiretapping, and mass data collecting. Provisions such as Section 201 enabled real-time monitoring through systems like the FBI's Carnivore Internet Filtering System, bypassing prior judicial authorization [41]. These capabilities made the extensive use of surveillance equipment possible, decreasing judicial oversight and accountability and raising concerns about privacy erosion and abuse. Section 215 allowed for the acquisition of business records from service providers without establishing probable cause, while National Security Letters (NSLs) permitted the government to obtain customer data without a judge's consent. The use of wiretappings was also extended to foreign intelligence content. As a result, the government was not obligated to approach the Court with the intent to obtain permission for surveillance, exhibiting the use of the communication channel by the targeted person. Before the Act was passed, it was required to present evidence to regulate the surveillance of communications for foreign intelligence. The Act also allows NSLs to obtain customer records without a judge's consent. Even foreign nationals suspected of terrorism can be monitored by the government, even if they have tenuous connections to terrorist groups. The Act's broad powers and ambiguous language caused it to be hard to distinguish between criminal investigations and intelligence, raising serious concerns about government abuse and putting constitutional privacy protections at risk.[42]

The post-9/11 surveillance regime, exemplified by expansive laws such as the USA PATRIOT Act, normalized mass surveillance and significantly reduced judicial scrutiny. However, the full scale and intrusiveness of these practices remained obscured from public view until 2013. That year marked a critical inflection point when Edward Snowden's disclosures provided unprecedented insight into the scope of global

[39]David Lyon, Electronic Surveillance and Privacy in the United States After September 11, 11 INT' L J. Info. Ethics 7 (2004).
[40]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272
[41]Paul Rosenzweig, The USA Patriot Act and Privacy: A New Frontier of Surveillance, 13 STAN. TECH. L. REV. 1 (2010).
[42] David Harrington**,** U.S. Privacy Laws: The Complete Guide, VARONIS (n.d.), https://www.varonis.com/blog/us-privacy-laws#us-data-privacy-law-timeline.

surveillance, confirming long-standing fears about unaccountable state power and catalysing a wave of global outrage and reform initiatives.

2.8 Snowden Revelations and Global Backlash

The extent of such overreach became evident in 2013 when Edward Snowden, American technologist, former CIA officer, and National Security Agency contractor, leaked classified documents detailing mass surveillance programs. This conduct goes against its public statements and violates human rights standards and international law. State surveillance and citizens' right to privacy have been at the centre of international debate after the explosive Snowden disclosures in May 2013. Snowden's documents reveal the breadth and depth of intelligence agencies' extensive surveillance systems (PRISM and TEMPORA, among others) undertaken by the U.S. National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), and other states' intelligence apparatuses which is used to spy both on their citizens and upon communications elsewhere.[43]

Following these disclosures, public society and governments were forced to confront difficult questions like, How much surveillance is excessive?, Whether intelligence agencies have unrestricted power?, How can we ensure democratic oversight? The worldwide conversation on government openness, digital privacy, and the obligations of tech companies to protect user data was eventually altered by the Snowden leaks[44].

The revelations brought forth by Snowden sparked not only widespread public debate but also spurred legislative responses aimed at curbing unchecked surveillance and reinforcing individual data rights. Among the most notable of these developments was the European Union's General Data Protection Regulation (GDPR), which emerged as a comprehensive framework seeking to restore control to individuals over their personal data. In many ways, GDPR represented a normative shift transforming privacy from a

[43] Ashley Deeks**,** An International Legal Framework for Surveillance, 55 VA. J. INT'L L. 291 (2015)
[44] Gautham Batia, Supra Note 3

passive entitlement into an enforceable right backed by stringent legal obligations for both public and private entities.[45]

2.9The Global Standard: GDPR and Its Influence

Since the amount of personal data being shared online has increased significantly, regulatory frameworks are now required to safeguard users' rights and stop misusing sensitive data. One of the most comprehensive and influential data protection laws is the General Data Protection Regulation (GDPR)**,** which came into effect in the European Union (EU) in 2018. The GDPR establishes strict rules on how organizations collect, store, process, and share personal data. GDPR applies to any organization that processes or intends to process EU citizens' sensitive data, regardless of location. GDPR compliance is mandatory for any organization that processes the personal data of EU citizens, regardless of whether they are customers or not. Certain fundamental rights are granted to individuals, such as the opportunity to access their data, the right to be forgotten, and data portability, which allows users to move their data between service providers. The regulation has set a global standard, influencing privacy laws in other regions and prompting businesses worldwide to adopt more transparent data practices[46].

2.10 Conclusion

Individual autonomy and dignity are foundational to the concept of the right to privacy. It is a fundamental aspect of human freedom essential to preserving one's integrity and dignity; it is not only a legal notion. In early times, societies usually functioned on a collective structure where the needs of the society took precedence over the subjects' privacy. As a result, privacy was not acknowledged as an essential right. However, the necessity of privacy became widely recognized when societies started to develop. In the present scenario, many legal system across the globe have accepted privacy as a fundamental right

[45] Agustín Rossi, How the Snowden Revelations Saved the EU General Data Protection Regulation, 53 INT'L SPECTATOR 116 (2018).
[46] Paul Voigt & Axel Von Dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer 2017).

However, conventional privacy ideas have been questioned by the quick development of technology, globalization, and heightened government surveillance. While individual liberty and privacy remain fundamental principles of democratic countries, sustaining this equilibrium has become more difficult due to the necessity of public safety and national security.

Governments and security agents argue that access to specific personal data is necessary to maintain law and order, combat terrorism, and anticipate potential hazards. However, there is a risk that uncontrolled surveillance and data collection methods might erode democratic freedoms, suppress dissent, and violate civil liberties.

CHAPTER 3

JUDICIAL OVERSIGHT AND THE RIGHT TO PRIVACY IN INDIA

3.1 Introduction

The preamble of the Indian Constitution ensures citizens' liberty of thought, expression, belief, faith, and worship. A main aspect of this liberty is enshrined in Article 21[47], which safeguards an individual right to life and personal liberty. The notion of "Personal Liberty" within Article 21 emphasizes the necessity of safeguarding individual autonomy and dignity, thereby rendering the legal recognition of the right to privacy. This right is intrinsic to human dignity and serves as a cornerstone of an individual ability to lead a purposeful and autonomous life[48]. Article 21, often regarded as the heart and soul of the Indian Constitution, extends beyond mere existence and encompasses all elements essential to a dignified life, including privacy, personal autonomy, and freedom from unwarranted intrusions. It establishes a fundamental safeguard against state and non-state actors encroaching upon the private domain of individuals, protecting crucial aspects of personal identity.

The right to privacy, carries both negative and positive dimensions: while it shields individuals from arbitrary state interference, it also places an affirmative obligation on the state to create an environment where individuals can freely shape their identities[49]. Despite its implicit presence within the constitutional framework, the right to privacy was not explicitly recognized as a fundamental right at the time of the Constitution's adoption. Its legal recognition have primarily evolved through judicial interpretation[50]. The judiciary has played a pivotal role in defining the contours of privacy, addressing

[47] India Const. art. 21
[48] Kush Kalra, Right to Privacy Under Indian Constitution, 2 GIBS L.J. 38 (2020)
[49] Anna Jonsson Cornell, Right to Privacy, in Max Planck Encyclopedia of Comparative Constitutional Law (Rainer Grote, Frauke Lachenmann & Rüdiger Wolfrum eds., Oxford Univ. Press 2020).
[50] Tejas Jindal, Right to Privacy as a Fundamental Right in India: Evolution, Challenges and the Impact of Digitalization, Int'l J. for Multidisciplinary Res., Nov.–Dec. 2024, at 1.

its implications in various spheres, including personal liberty, state surveillance, and data protection.

3.2 Origin

The concept of privacy is not unknown to Indian society. We can trace it to the ancient texts of Dharmashastras and Hitopadesha. The laws of privacy have been outlined in commentaries on Dharmashastras. According to Hitopadesha, certain matters like sex and family should be kept private. Be it in Upanishad, Manu Smirti, or Vedic; privacy has been considered an essential part of individual life so, looking from the historical point of view, early code creators considered privacy to be part of civil liberty, which is indispensable to the freedom and dignity of an individual[51].

Towards the half of the 20th century, India became independent. When the Constitution of India was framed, it can be noted that the right to privacy was not explicitly highlighted within the list of fundamental rights to be conferred to the citizens of India, even though debate and discussion have taken place in the constituent assembly about privacy.

In December 1946, the Constituent Assembly started the formal proceeding of drafting the Constitution, and the Constituent Assembly constituted various committees whose role was to provide reports to the Drafting committee, which would, in turn, formulate a draft of the Constitution[52]. The formal proceeding of the Constituent Assembly started with the drafting in December 1946, and the Constituent Assembly constituted various committees whose main work was to provide reports to the Drafting committee, which would, in turn, formulate a draft of the Constitution. At the Committee Stage, a Subcommittee group attempted to support including the right to privacy in the list of fundamental rights. During the various meetings, distinguished members like K.M. Munshi, Harman Singh, and Dr. Ambedkar strongly promoted the incorporation of the right to privacy as one of the fundamental rights, and this thought was reflected in Dr. B.R. Ambedkar's draft, which proposed a provision stating 'the right of the people to be secure in their persons, house, papers and effects against unreasonable searches and seizures shall not be violated and no warrants shall issue but upon probable cause,

[51] Sargam Thapa, The Evolution of Right to Privacy in India, 10 INT'L J. HUMAN. & SOC. SCI. INVENTION, Feb. 2021
[52] Id.

supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized' in the State and Minority Report[53].

However, from the initial stage itself, there were substantial differences of opinion related to the right to privacy members like B.N Rau, A. K Ayyar ,M.K. Panikkar, and Alladi Krishnaswami Ayyar who strongly objected to giving the right to privacy status as a fundamental right. A. K. Ayyar believed that providing the right to privacy would be detrimental since it would make all civil and private communications equal to state documents. B.N. Rau thought that grant of a right of privacy would interfere with the police investigation Later, Rau and Ayyar persuaded the Advisory Committee to opt out of provisions concerning the right to privacy. So, the Advisory Committee's final report did not mention anything related to the right to privacy.

On 30th April 1947, Somnath Lahiri, one of the members of the constituent assembly, presented a proposal to make the right to privacy of correspondence a fundamental right,'the privacy of correspondence shall be inviolable and may be infringed only in cases provided by law..' [54]. However, it failed to get a favourable response. After almost a year another, i.e., in 1948, another member of the constituent assembly, Kazi Syed Karimuddin, tried to incorporate this idea and to support his proposal, he relied on Article 4 of the American constitution, Clauses 2,5 of the Irish constitution, and Articles 114 and 115 of the German constitution, which provide similar kinds of rights to their citizen. However, this proposed amendment could not garner any support. So, the Indian Constitution failed to recognize the right to privacy as a part of the fundamental rights conferred to the citizens of India[55].

After its independence, India signed two international treaties to protect human rights. The first is the Universal Declaration of Human Rights, and the other is the Covenant on Civil and Political Rights. United Nations Organization (UNO) adopted the Universal Declaration of Human Rights in 1948. Under this document, the right to privacy is recognized as a foundational right, and it is the obligation of members who have signed it to protect the right to privacy of their citizens through their municipal

[53] B.R. Ambedkar, State and Minorities: Article II Section I – Fundamental Rights of Citizen, SM.23 (1947).
[54] Constituent Assembly of India Debates, vol. 3, at 451 (Apr. 30, 1947), https://www.constitutionofindia.net/constitution_assembly_debates/volume/3/1947-04-30.
[55] Constituent Assembly of India Debates, vol. 7, at 882 (Dec. 3, 1948), https://www.constitutionofindia.net/constitution_assembly_debates/volume/7/1948-12-03#7.66.11

laws. Another treaty for protecting Human rights adopted by UNO is the International Covenant on Civil and Political Rights 1966 (ICCPR, 1966). It has also recognized the right to privacy as a fundamental right. Being a signatory of the above international treaties, India's obligation is to protect citizens' right to privacy. Despite being a member of international treaties, India has still not enacted laws to protect the right to privacy[56].

3.3Judicial Oversight

Over a period of time none other than the Supreme Court of India has played an important role to addressed a number of cases that has dealt with right to privacy in some form or the other and which has helped the right to privacy attain its rightful position as a part of Right to Life and Liberty under Article 21. The Article states, "No person shall be deprived of his life or personal liberty except according to procedure established by law." The dimension of Article 21 has widened by giving extended meaning to the words life and liberty. The Supreme Court of India has asserted that Article 21 of the Indian Constitution is the core of the Fundamental Rights. Some landmark cases can be enumerated forthwith to trace the evolution of right to privacy here as under:

1. ***M.P. Sharma v. Satish Chandra (1954)***[57]

This case is one of the fundamental judgments of the Supreme Court concerning the right to privacy in India. In 1952, the company went bankrupt due to embezzling funds and was accused of falsifying accounts to mislead shareholders. In 1953, an FIR was filed, leading to a search warrant during the course, and records were seized. The petitioner challenged the fact that the searches violated the petitioners' fundamental rights. The Court dismissed the Petitioners' argument emphasizing the State has overriding power to regulate searches for societal security and noted that, unlike the US Constitution's Fourth Amendment, the Indian Constitution did not expressly recognize the right to privacy, and there was no justification to import such a right through interpretation.

[56] Ramakant Tripathi**,** Evolution of Right to Privacy in India: National and International Perspective, 7 J. CRIT. REV. 300 (2020).
[57] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

2. Kharak Singh v. State of U.P , (1963)[58]

In this case, Kharak Singh, petitioner, had been charged with violent robbery as part of an armed gang in 1941 but he was released due to lack of evidence, but a 'history sheet' was opened in regard to him under the Uttar Pradesh Police Regulation 236, which provided for surveillance powers, including powers of domiciliary visits, for habitual offenders or people likely to become criminals. The petitioner's challenges centres on the constitutional scrutiny of the Uttar Pradesh Police Regulations. He contended that surveillance of the police officers effect his fundamental right guaranteed under article 21 of the constitution i.e Right to Life, which implied the right to life with human dignity and not mere animal existence. The six judge Supreme Court panel held that Regulation 236 (b) which authorises "domiciliary visits" is unconstitutional and struck down however with respect to right to privacy the court held that the right to privacy is not a guaranteed right under the Constitution.

3. *Govind v. State of M.P, (1976)* [59]

This case is similar to the earlier case of Kharak Singh v State of Uttar Pradesh, whereby the petitioner, Govind, filed *a* writ petition before the SC challenging the validity of Regulations, mainly regulations 855 and 856 of the Madhya Pradesh Police Regulations made by the Government under the Police Act, 1961 (Police Act) which permitted domiciliary visits and other forms of surveillance of individuals with a criminal background. The petitioner contended that due to the false allegation based on several criminal cases filed against him, he had been deemed a habitual offender, and because of this, the police had opened a history sheet, and he was being consistently surveilled. The police had been frequently visiting his house and secretly picketing his house. He argued that such surveillance violated his fundamental rights under Articles 19(1)(d) and 21 of the Constitution. In this case, The three judges Bench of the Apex Court considered the matter in detail and adverted to its earlier decision in Kharak Singh's case[60]. The court acknowledges there exist an implied right to privacy, but such a right is not absolute and can be restricted by law for state interest. This means that if the surveillance is for a legitimate purpose, even if it violates an individual's privacy rights,

[58] Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[59] Govind v. State of M.P., AIR 1975 SC 1378.
[60] Kharak Singh v. State of U.P., AIR 1963 SC 1295

it can be justified unless such surveillance should not be unnecessarily vexatious or humiliating.

4. *Malak Singh v. State of Punjab (1981)*[61]

In this case, the provisions of Section 23 of the Punjab Police Rules were challenged before the Supreme Court, under which the surveillance register was maintained in accordance. The appellants claimed that they had been falsely alleged to be part of some criminal cases due to political enmity with a Congress MLA. Since their name was entered into the surveillance register, they were frequently monitored by the police officers and harassed by being called to the police station. The petitioner filed a special leave petition before the Supreme Court since the High Court of Punjab and Haryana dismissed the writ petitions filed by the Appellants, Malak Singh and Jaswant Singh, who were seeking the removal of their names from the surveillance register maintained with the police.

The SC remarked that the prevention of crime is the utmost thing, and the means of preventing crime must be within the boundary of fundamental rights guaranteed under Article 19(1)(d) and Article 21 of the Constitution. The Court tried to strike a balance between the two interests, ruling that it is necessary to monitor habitual offenders to prevent crime, however, such surveillance could not be so intrusive that it infringes upon constitutionally guaranteed freedoms, including the right to privacy. The Court even cited Article 8 of the European Convention on Human Rights[62] order to reinforce the need to protect private and home life and, therefore, personal dignity and liberty. The Court, however, did not consider conducting surveillance as unlawful but observed it should be permissible surveillance only to the extent of a close watch over the movements of the person under surveillance and no more. Surveillance must strictly be of people who were legitimately listed in the surveillance register and for crime prevention. Excessive surveillance falling outside the ceiling prescribed by the Rules would entitle a citizen to the Court's protection.

[61] Malak Singh v. State of Punjab, (1981) 1 SCC 420.
[62] European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221

5. R. Rajagopal v State of Tamil Nadu, (1995) [63]

This case is a landmark judgment pertaining to the right to privacy and freedom of speech and expression. This case revolves around the publication of the autobiography book of the prisoner Shankar, who was awarded the death penalty for murder. His autobiography exposes the illegal ties between senior prison authorities and state officials. Before his death, he entrusted the book to his wife and instructed her to publish it in Nakeeran magazine. Upon learning this, the Inspector General of Prisons warned the petitioners, claiming the book was defamatory and threatened legal action. Fearing interference, they filed a suit under Article 19(1)[64] to safeguard press freedom, but the High Court dismissed it. They then appealed to the Supreme Court under Article 32[65] to restrain the authorities from blocking the publication. The petitioner contented that every individual has the fundamental right to express their views and argued the prisoner had the right to publish book under article 19(1)(a)[66]. They claimed state officials sought to suppress the book out of fear of exposure. In Addition, petitioner contended that, the right to privacy was not a fundamental right at that time, making freedom of speech take precedence based on the issue's significance. The Supreme Court ruled that the prisoner had full rights to publish his autobiography, and the publisher could do so freely. The Court affirmed that publishing about Shankar was permissible as it fell under public records, requiring no prior consent. Citing Kharak Singh[67] and Govind cases[68], the Court recognized privacy as implicit under Article 21 but not absolute, have to go through a process of case-by-case development. It also held that public officials cannot sue for defamation over acts performed in official duties unless proven false. No law permits officials to impose unwarranted restrictions on the press.

6. *Peoples' Union for Civil Liberties v. Union of India (1997)* [69]

This case is also known as "phone tapping case" , in this case the SC considered the issue pertaining to phone tapping. The People's Union of Civil Liberties (PUCL)

[63] R. Rajagopal v. State of T.N., (1994) 6 SCC 632.
[64] India Const. art. 19.
[65] India Const. art. 32.
[66] India Const. art. 19(1)(a)
[67] Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[68] Govind v. State of M.P., AIR 1975 SC 1378.
[69] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

challenged the validity of Section 5(2) of the Indian Telegraph Act of 1885.[70] The SC affirmed that telephone tapping infringed on the right to privacy, which is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution and infringement of the constitutional guarantee of free speech and expression enshrined under Article 19(1) (a) unless authorized by Article 19(2). The court further relied on Article 17 of the International Covenant on Civil and Political Rights and a similar guarantee under Article 12 of the Universal Declaration of Human Rights, which protects privacy. However, the court hesitated to strike down the section as unconstitutional. Instead, the court stressed that there is a need for the executive to adhere to the two statutory pre-conditions for the exercise of the power to interpret: "occurrence of any public emergency" or "the interest of public safety". The PUCL Court also laid down detailed safeguards designed to check arbitrariness in the issuance of telephone tapping in exercising the state's surveillance powers.

1. Orders for telephone tapping may only be issued by the Home Secretary of the central government or a state government. In an emergency, this power may be delegated to an officer of the Home Department of the central or state government, and a copy of the order must be sent to the concerned Review within one week.
2. The authority making the order must consider whether the information that is considered necessary to acquire could reasonably be acquired by other means.
3. Orders issued under the Indian Telegraph Act of 1885 shall be valid for two months from the issue date.
4. Review Committees shall consist of Secretary-level officers at the central and state levels. They may evaluate whether an interception order has been passed in

[70] Indian Telegraph Act, 1885, Sec 5(2): Power for Government to take possession of licensed telegraphs and to order interception of messages.--(2) On such occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought by transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:
Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

compliance with the law. If it has not, they may set it aside and direct the destruction of any copies of the intercepted communications.

5. The authority issuing the interception order must maintain records of (i) the intercepted communications, (ii) the extent to which material is disclosed, (iii) the number of persons to whom the material is disclosed and their identity, (iv) the extent to which the material is copied; and (v) the number of copies made (each of which must be destroyed as soon as its retention is no longer necessary).

This is a landmark judgment as it laid down procedural safeguards for the protection of the right to privacy of a person until Parliament frames the rules under Section 7 of the Indian Telegraph Act of 1885. In this way, the Apex Court has tried to fill up the void of matching procedural law about the substantive law in Section 5 (2) of the Indian Telegraph Act, 1885. Later the PUCL guidelines were substantially modified and codified under Rule 419-A of the Indian Telegraph Rules, 1951.

7. State of Maharashtra Vs. Bharat Shantilal Shah (2008) [71]

In this case, The petitioner first brought the petition before the Bombay High Court, challenging the constitutional validity of, particularly the provisions of Sections 2(d), (e), and (f), Section 3, Section 4, Sections 13 to 16, and Section 21(5) of the MCOCA **(**Maharashtra Control of Organized Crime Act). Sections 2, 3, and 4 deal with the definition of 'organized crime' and the award of punishments. Sections 13 to 16 empower the State Government to appoint a competent authority for approving, reviewing, and restricting the disclosure of intercepted communications in organized crime investigations. Section 21(5) denies bail to an accused if he was on bail for an offense under the MCOCA Act or any other act at the time of the commission of the alleged offense.

The Bombay High Court upheld the validity of Sections 2(d), (e), and (f), Section 3, and Section 4. It struck down Sections 13 to 16 as well as Section 21(5) for being unconstitutional as the Court ruled that it was beyond the legislative competence of the State Legislature and the provisions violate fundamental rights guaranteed under Article 14. Aggrieved by the decision of the Bombay High Court, the Appellant, i.e., the State of Maharashtra, filed an appeal in the Supreme Court.

[71] State of Maharashtra v. Bharat Shantilal Shah, (2008) 13 SCC 5.

The Appellant argued that the provisions of MCOCA define organized crime, and for detection and investigation of such offenses, interception of wire, electronic, and oral communication was necessary to prevent the commission of an organized crime or to collect the evidence of such an organized crime. The State government also contended that the grounds for interception of communication under MCOCA differed from those under the Indian Telegraph Act of 1885. It also submitted that the provisions of the MCOCA were legally valid under Entries 1 and 2 of List II and Entries 1, 2, and 3 of List III of the Seventh Schedule, advocating for a broad interpretation of these entries.

The Supreme Court upheld the constitutionality of Sections 2(d), (e), (f), 3, and 4 of MCOCA. However, it struck down the words "or under any other Act" in Section 21(5), ruling that restricting bail for unrelated offenses created an unreasonable classification, violating Articles 14 and 21. About sections 13- 16, the Court examined legislative powers by applying the pith and substance doctrine and presumption of constitutionality. It ruled that MCOCA's interception provisions differed from the Telegraph Act and, despite incidental encroachment on Union List matters, MCOCA remained within the State Legislature's authority. The Court also analysed whether these provisions violated the right to privacy under Article 21 and held that the interception of conversation constitutes an invasion of an individual right to privacy, but the said right could be curtailed by the procedure validly established by law. Thus, the Court must see that the procedure must be fair, just, reasonable, non-arbitrary, fanciful, or oppressive.

8. *Selvi and Ors. v. State of Karnataka (2010)* [72]

The case, Selvi and Ors. v. The State of Karnataka addressed the constitutionality of using scientific techniques like narcoanalysis, polygraph tests, and brain mapping (Brain Electrical Activation Profile or BEAP) to gather evidence in criminal investigations. In 2004, Selvi and others filed a criminal appeal, followed by more appeals until 2010, consolidated by the Supreme Court under a special leave petition in May 2010. The petitioner challenged the involuntary use of tests on accused persons, suspects, or witnesses. The state argued that these tests are essential for collecting vital evidence from suspects in complex cases; it also argued that these tests do not violate

[72] Selvi v. State of Karnataka, AIR 2010 SC 1974.

the right against self-incrimination and did not require the accused to provide written or spoken remarks; they did not breach the right against self-incrimination. Further arguing that they were harmless, aided investigations, and were more humane than coercive interrogation methods.

The chief justice of India, K.G. Balakrishnan, declared the involuntary administration of narcoanalysis, polygraph, and brain mapping tests unconstitutional, violating the right against self-incrimination (Article 20(3))[73]. The right to life and personal liberty (Article 21), and the court ruled that the results obtained from these tests are testimonial and cannot be categorized as material evidence.

9. Amar Singh V. Union of India (2011)[74]

This case deals with the constitutionality of phone tapping. In this case, the Petitioner, Amar Singh, learned that his phone conversation was being recorded by the telecom service provider, Reliance Info com Ltd., Delhi, on the behest of a request allegedly issued from the office of the Joint Commissioner of Police. This was followed by an official authorization of the request from the Principal Secretary (Home) of the Government of NCT of Delhi. He believed that the wiretapping was being done because of the political positions he held. Following this, he approached the Supreme Court to declare the wiretapping unconstitutional and an infringement upon his right to privacy. He sought a declaration of the interception orders as unconstitutional, disclosure of details, guidelines for phone interceptions, a judicial inquiry, and damages.

The government, however, stated that the interception request was forged and fabricated, and a criminal case for forgery was already underway. It asserted that no valid request was made by the Joint Commissioner of Police, and the Home Department could not have initiated it independently. Errors in the request further indicated its inauthenticity.

The three-judge bench observed that while service providers were rightly under the duty to act promptly on a request received from Government agencies for interception, they were equally duty bound to verify the authenticity of such communication immediately. The Court ruled that Sanctity and regularity in official communication in such matters

[73] India Const. art. 20(3)
[74] Amar Singh v. Union of India**,** (2011) 7 SCC 69.

must be maintained especially when the service provider is taking the serious step of intercepting the telephone conversation of a person and by doing so is invading the privacy right of the person concerned and which is a fundamental right protected under the Constitution, as has been held by this Court. The telecom service provider's failure to verify the authenticity of a suspicious request meant that it had failed in its public duty. The Court dismissed the petition for being frivolous and speculative. However, the Court gave the Petitioner the liberty to seek appropriate legal remedy against the telecom service provider for unauthorized interception. It directed the Central Government to frame guidelines regarding the interception of phone conversations.

***10. Ramlila Maidan Incident Vs. Home Secretary, Union of India*[75]**

The Supreme Court in this case recognized privacy and dignity as fundamental human rights, akin to freedom of speech and association. It held that any act impairing human dignity violates the right to life under Article 21, and state actions must be reasonable, fair, and just. The Court observed that the right to privacy is implicit in Article 21, protecting individuals from unlawful intrusions, and extended this right even to women of easy virtue. However, it clarified that the right to privacy is not absolute, and in exceptional cases, lawful surveillance under statutory provisions may be permissible.

***11. Unique Identification Authority of India & Anr. v. Central Bureau of Investigation(2014)*[76]**

The Central Bureau of Investigation (CBI) was investigating a serious criminal case involving the rape of a minor girl in Goa. During the investigation, the CBI obtained fingerprints from the crime scene and sought access to the Aadhaar database maintained by the Unique Identification Authority of India (UIDAI) to identify the perpetrator. The UIDAI declined to share the biometric data, citing concerns over privacy and the absence of explicit consent from individuals.

Subsequently, the CBI approached the Magistrate Court, which directed the UIDAI to provide the requested data. The UIDAI challenged this order before the Bombay High Court at Goa, which upheld the Magistrate's directive. Aggrieved by this decision, the

[75] Ramlila Maidan Incident v. Home Secretary, Union of India, AIR 2011 SC 3973
[76] Unique Identification Authority of India & Anr. v. Central Bureau of Investigation, Crim. Appeal No. 2524 of 2014

UIDAI filed a Special Leave Petition before the Supreme Court. The SC, passed an order which reads as follows: "No person shall be deprived of any service for want of Aadhaar number in case he/she is otherwise eligible/entitled. All the authorities are directed to modify their forms/circulars/likes so as to not compulsorily require the Aadhaar number in order to meet the requirement of the interim order passed by this Court forthwith. Also the UIDAI was restrained from transferring any biometric information of Aadhaar holders to any other agency without the individual's written consent. The Supreme Court stayed the operation of the Bombay High Court's order that had directed the UIDAI to share biometric data with the CBI.

12. *Justice K.S. Puttaswamy v. Union of India (2017)*[77]

The case of Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. stands as a defining moment in India's privacy jurisprudence. The Supreme Court, for the first time, unequivocally declared privacy as a fundamental right .The Supreme Court, in a landmark nine-judge bench decision, affirmed that privacy is a fundamental right under the Constitution of India. However, this right is not absolute and may be restricted if such limitations are prescribed by law, serve a legitimate state aim, and are proportionate to the objective sought to be achieved. The Judgment was in response to the reference made in connection with the challenge to India's National Identity project called Aadhar. The advocate General of India had argued that the Indian Constitution does not include within it Fundamental Right to privacy and he had placed this argument on the basis of two earlier cases, the first was the M.P. Sharma vs. Satish Chandra[78] that was decided by a eight Judge bench in the year 1954 and the second case was Kharak Singh vs. State of U.P[79] that was decided by Six Judge bench in the year 1962 and both of these cases at different point had stated that there is no provision in the Indian Constitution that will protect the right to privacy. The Court overruled both decision that had previously held that privacy was not constitutionally protected. The judgment extensively analyzed international and regional privacy laws, foreign rulings, and concepts such as informational privacy. Justice Chandrachud, writing for the plurality, emphasized that the right to privacy is intertwined with other liberties

[77] Justice K.S. Puttaswamy v. Union of India**,** (2017) 10 SCC 1
[78] M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300
[79] Kharak Singh v. State of U.P., AIR 1963 SC 1295.

enshrined in Part III of the Constitution, viewing it as an inalienable natural right and an essential component of human dignity. The Court specifically addressed the challenges posed by informational privacy, recognizing that technological advancements have transformed how personal data is collected and utilized. The internet, social media, and digital services have led to an interconnected world where personal information is continuously generated and stored. The Court observed that activities such as online banking, e-commerce, instant messaging, and internet browsing leave electronic footprints that can be exploited without the user's knowledge. Websites and digital platforms use cookies, algorithms, and automated content analysis to track user behaviour, target advertisements, and build consumer profiles, thereby subjecting individuals to digital surveillance. This growing concern over data privacy and unauthorized data mining led the Court to stress the importance of safeguarding personal information and maintaining a delicate balance between state interests and individual rights.

The judgment also addressed the role of data regulation in ensuring privacy protection. The Court noted that while state intervention in data privacy is sometimes necessary, it must be carefully regulated to prevent excessive encroachment on individual freedoms. The government informed the Court about the formation of a committee chaired by Justice (Retd.) B.N. Srikrishna to review data protection norms and propose legislation for safeguarding privacy. The committee later submitted its report in July 2018, which played a key role in shaping India's evolving data protection framework.

13. C. P. Girija v. Superintendent of Police, 2021[80], wp no. 37089

In this case, the petitioner filed a writ petition under Article 226 of the Constitution, seeking to forbid the respondent police authorities from frequently interfering with the lawful business activities of the petitioner, who is running an Ayurvedic spa center, which causes disturbances resulting in prejudice to the business operations. However, in this case, the Madras High Court opined that there are many allegations against such spa centers and massage centers in the public domain that these are the places where prostitution happens, so if any such doubt arises, the Police officers are obligated to conduct inspections in order to verify the business activities and to prevent illegal

[80] C.P. Girija v. Superintendent of Police**,** W.P. No. 37089 of 2021.

activities in the premises. The court held that the claim made by the petitioner that they are conducting lawful business cannot always be trusted, and Police authorities are duty bound to verify the same to ensure such lawful business in that locality. The court directed the police authorities to issue appropriate orders to all spa and massage centres across the state to install functional CCTV cameras. Also, issue pertinent direction to ensure that these centre lawfully conduct their business, showcasing transparency and avoiding closed rooms that facilitate illegal activities. In the event of reasonable suspicion or any such complaint or information is received, the police authorities are directed to take all appropriate actions as per the law**.**

14. *Payel Biswas v. The Commissioner Of Police ,2022*[81]

In this case, the petitioner files a Writ Petition under Article 226 [82]of the Constitution of India to issue a Writ of Mandamus to direct the second respondent to issue a No Objection Certificate to the petitioner to run a "SPA" centre. Initially, no law regulated such businesses, but the state had issued a notification that made it mandatory to obtain a license. The petitioner applied for the same, but no action was taken regarding his request. So he filed a writ petition to the High Court of Madras to direct the police officers to issue a "no objection certificate." He also pleads with the Court to restrain the unlawful interference from the side of police authorities. The Court held that the judgment in C.P Girija v The Superintendent of Police and Others[83] appears to run counter the law laid down by the 9-judge bench judgment of the Supreme Court in K.S Puttaswamy v. Union of India under Article 21 of the Constitution which guarantees to all persons the fundamental right to privacy. Justice Swaminathan opined that privacy, as guaranteed in Article 21 of the Constitution, takes different forms, like the right to bodily autonomy, informational privacy, and privacy of choice. The installation of CCTV equipment inside premises such as a spa would unquestionably infract upon a person's bodily autonomy. While the government can regulate businesses, it cannot impose privacy intrusive measures without legislative backing; existing regulations only require CCTV at entry and exit points, not inside treatment rooms. The Court referred to previous judgments, such as Masti Health and Beauty Pvt. Ltd. v.

[81] Payel Biswas v. The Commissioner of Police, W.P. (MD) No. 7680 of 2021.
[82] India Const. art. 226.
[83] C.P. Girija v. Superintendent of Police**,** W.P. No. 37089 of 2021.

Commissioner of Police, Chennai City[84], which stated that police could not interfere in spa centres unless there is concrete evidence of unlawful activities. Consequently, the Commissioner of Police, Trichy, was directed to decide on the petitioner's NOC application within four weeks. If granted, the police must not interfere as long as the spa operates lawfully. The Court rejected mandatory CCTV installation inside spa rooms, upholding privacy rights.

15. *Ms. Aaradhya Bachchan v. Bollywood Times & Others*, 2023[85]

In this case , the Delhi High Court strongly reaffirmed the sanctity of the right to privacy, particularly that of a child, as an essential facet of Article 21 of the Constitution. The case arose when false and morbid videos were circulated on YouTube, falsely asserting that the minor petitioner, daughter of Abhishek and Aishwarya Bachchan, was critically ill or deceased, accompanied by morphed images designed to lend credence to these fabrications. The Court unequivocally held that such acts constitute an egregious invasion of the petitioner's privacy and dignity, underscoring that every child, regardless of celebrity status, is entitled to be treated with honour and respect, free from unwanted public scrutiny. The judicial holding emphasized that the right to privacy is not a luxury but a fundamental entitlement, more so in the case of minors who are vulnerable to digital exploitation.

To summarize, the evolution of right to privacy it can be said that after a very long legal interpretation that has been laid down by the Supreme Court at various point of time, it is adequate enough to come to a conclusion that the Right to Privacy has finally been incorporated into the Part III of the Indian Constitution. Privacy can also be considered to be one of the features of the dignity of an individual and that is why, even the Preamble to the Constitution assures this to every individual person. The Right to Privacy is not just an apparatus in the hands of the State to trespass upon the personal space of the individual but it is also a mechanism through which the State can

[84] Masti Health and Beauty Pvt. Ltd. v. Commissioner of Police, Chennai City, W.P. No. 9380 of 2016.
[85] Ms. Aaradhya Bachchan v. Bollywood Times & Others, 2023 CS(COMM) 230/2023

adequately fabricate institutions that would allow every individual to protect his or her private life[86].

3.4 Right to Privacy not an Absolute Right, but is subject to reasonable restrictions

Privacy is the constitutional core of human dignity. Privacy safeguards individual autonomy and recognizes the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognizes the plurality and diversity of our culture. The right to privacy is fundamental to human dignity and personal liberty. It allows individuals to control their personal information, safeguard their autonomy, and make independent choices about their lives. However, like all fundamental rights enshrined in the Indian Constitution, the right to privacy is not absolute[87]. Any infringement of privacy must be by a law which is "fair, just and reasonable". Further, Article 19(2)[88] of the Constitution permits the state to impose reasonable restrictions on fundamental rights in the interests of sovereignty, security, public order, decency, or morality. In Govind v. State of M.P[89], the Court acknowledged that the right to privacy could be curtailed if there exists a compelling state interest or an important countervailing interest.

The landmark judgment in Justice K.S. Puttaswamy and Ors. Vs.Union of India and Ors. (2017)**[90]** firmly established the constitutional status of privacy while outlining the permissible restrictions that may be imposed on it. The Supreme Court acknowledged that it is not an absolute right. Any encroachment on privacy must pass a stringent three-fold test:

- The first requirement for a law to justify an encroachment on privacy is an express requirement of Article 21. No person can be deprived of his life or personal liberty

[86] Sargam Thapa, The Evolution of Right to Privacy in India, 10 INT'L J. HUM. & SOC. SCI. INVENTION, Feb. 2021
[87] Kush Kalra, Right to Privacy Under Indian Constitution, 2 GIBS L.J. 1 (2020).
[88] India Const. art. 19, cl. 2.
[89] Govind v. State of M.P., AIR 1975 SC 1378.
[90] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

except in accordance with the procedure established by law. The existence of law is an essential requirement.

- Second, the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness.
- The third requirement ensures that the means adopted by the legislature are proportional to the object and needs to be sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law.

Justice Chandrachud, in the judgment, stresses that the government must be held to high standards when they infringe on privacy by requiring the law, in itself, to be both specific and no broader than necessary to achieve legitimate objectives and that the principles of proportionality apply.

Justice Chelameshwar emphasized that privacy claims warranting the strictest scrutiny must meet the "fair, just, and reasonable" standard under Article 21, along with a "compelling state interest."

Justice Bobde affirmed that any infringement on privacy must adhere to the same test as restrictions on personal liberty, as established in Maneka Gandhi v. Union of India,[91] ensuring laws are fair, just, and reasonable, not fanciful, oppressive, or arbitrary.

Justice Nariman stated that statutory restrictions on privacy are valid if public or social interest outweighs individual claims.

Justice Sapre underscored that privacy is subject to reasonable restrictions based on social, moral, and compelling public interest.

Justice Kaul held that privacy would be subject to reasonable restrictions on national security, public interest, and the grounds enumerated in the provisos to Article 19 of the Constitution[92].

[91] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248
[92]Murni Wan Mohd ,Supra Note 31

However, in Anuradha Bhasin v. Union of India (2020)[93], the judiciary reaffirmed its stance on privacy when the Supreme Court examined the legality of internet shutdowns in Jammu and Kashmir. While the government justified the shutdown on national security grounds, the Court ruled that any restriction on fundamental rights, including privacy, must be "necessary and proportionate." This means that even national security cannot be used as an excuse for indefinite or excessive curtailment of rights. The judgment strengthened the principle that any government action affecting privacy must meet strict legal and constitutional standards.

Legislative frameworks such as Telecommunications Act of 2023, the Information Act of 2008 and the Digital Personal Data Protection Act of 2023 etc. give state the power of monitoring but certain legal justification is needed in order to protect national security and uphold public order under certain circumstances. Similarly In situations where individual acts or expressions might go against accepted norms of public morality or decency, the state has the power to regulate privacy[94].

Like other rights that form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty, Under Article 21, privacy is not an absolute right. A law encroaching upon privacy must withstand the touchstone of permissible restrictions on fundamental rights.

3.5 Conclusion

The right to privacy in India has witnessed a significant transformation from being excluded during the drafting of the Constitution to becoming a core component of the right to life and personal liberty under Article 21. Despite initial reluctance by the framers and judicial denial in early decisions such as M.P. Sharma v. Satish Chandra[95] and Kharak Singh v. State of U.P[96]., the idea of privacy gradually took root through a series of judgments that expanded the meaning of personal liberty.

[93] Anuradha Bhasin v. Union of India, A.I.R. 2020 S.C. 1308
[94] Tathagata Satpathy et al., Are India's Laws on Surveillance a Threat to Privacy?, The Hindu (Dec. 27, 2018), https://www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25844250.ece.
[95] M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300
[96] Kharak Singh v. State of U.P., A.I.R. 1963 S.C. 1295

Cases such as Govind v. State of M.P.[97], R. Rajagopal v. State of Tamil Nadu[98], and PUCL v. Union of India[99] laid the groundwork for recognising privacy in specific contexts. However, it was the landmark judgment in 2017 in Justice K.S. Puttaswamy v. Union of India[100] that firmly and unequivocally affirmed the right to privacy as a fundamental right, essential to dignity, autonomy, and individual freedom. The Court not only overruled prior decisions but also introduced a structured threefold test of legality, necessity, and proportionality for any permissible restriction on privacy.

The Court further acknowledged that in the context of technological advancement and data-driven governance, informational privacy is an evolving aspect of this right. Activities such as data collection, profiling, and digital surveillance were recognised as raising serious privacy implications, thereby necessitating a legal framework that balances state interests with individual rights[101].

At present, the right to privacy in India stands as a constitutionally protected and judicially enforced fundamental right under Article 21. Though not absolute, it enjoys the same constitutional status as other core freedoms and can only be restricted through a law that is fair, just, and reasonable, serving a legitimate public interest and proportionate to its aims. This recognition represents a decisive shift in Indian constitutional jurisprudence, aligning it with international human rights norms and ensuring that personal liberty is safeguarded in both physical and digital realms.

[97] Govind v. State of M.P., (1975) 2 S.C.C. 148
[98] R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632
[99] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301
[100] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1
[101] Mohd Faiz Khan & Dr. Naseem Ahmed**,** The Erosion of Privacy in the Face of State Surveillance: A Digital Dystopia, 29(1) MADHYA PRADESH J. SOC. SCI. 438 (2024).

CHAPTER 4

STATE SURVEILLANCE: AN OVERVIEW

4.1 Introduction

The debate over whether or not the nations have embraced surveillance technologies is over because both despotic and democratic governments use them. Autocratic nations like Saudi Arabia, China, and Russia use surveillance technologies to keep their people under control. These countries find surveillance technologies effective because once the citizens know that their movements are being monitored, they would alter their behaviour without any intervention from the government. On the other hand, democratic countries like India use surveillance technologies for national security and to improve public safety. However, at the same time, challenges arise in balancing state interests with individual interests. The political cultures of democratic nations, which are defined by their standards, values, and beliefs, are incompatible with the use of surveillance technologies against their population. In other words, the agreement between democratic governments and their citizens to guarantee civil liberties and privacy conflicts with monitoring technologies. Democratic states must take immediate action to settle this dispute because the unheard speed of technological advancement is creating a division between how these governments and their populations see their own political cultures.[102]

4.2 State Surveillance

Surveillance is derived from the French word Surveil, meaning to "watch over". It entails close observation of an individual or a group of individuals, particularly ones whom law enforcement agencies suspect as 'the act of carefully watching someone or something, especially to prevent or detect a crime.'[103] According to David Lyon, a key

[102] Torin Monahan, "Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance," in Surveillance and Democracy, (2010)
[103] Maja Galic, Surveillance and Privacy in Smart Cities and Living Labs: Conceptualising Privacy for Public Space (2019)

surveillance theorist, surveillance is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction. Haggerty and Ericson define surveillance as collecting and analysing population information to govern their activities. Surveillance is intrinsically ambiguous. This surveillance method of individuals and organizations goes back to ancient civilizations, when officials read specific individuals' letters to learn more about their goals. In addition, foreign guests were kept under close surveillance so that they would not do anything harmful to the state's interests[104].

The advancement of surveillance technology reached its pinnacle in the twentieth century, particularly during the Cold War era. During this era, the term surveillance also includes observation from a distance by electronic equipment such as closed circuit television or interception of electronically transmitted information such as Internet traffic or Phone calls.[105]

In the wake of technological advancements, interception jurisprudence, which has focused on targeted surveillance for years, has been replaced mainly by mass surveillance. Mass surveillance operates very differently from targeted surveillance. Mass surveillance is commonly understood as 'passive' or 'undirected' surveillance. It is not targeted at any particular person, but rather it collects data for future use. States have bulk access to communication content and related information and can mine all communication data for specific keywords or other information that might result in the identification of targets. So in today's world, most surveillance technologies are not applied to suspected persons but indiscriminately and to everyone in all contexts all places, times, networks, and groups of people[106]. Carrying out mass surveillance is justified by governments as necessary to empower them to combat the myriad threats posed by criminal and terrorist organizations, which have benefited from sophisticated technologies. It can cause harm to society in novel, unpredictable, and undetectable ways.[107]

[104] Anri Nishnianidze, Surveillance in the Digital Age, EUR. SCI. J., Feb. 2024
[105] Id.
[106] Chinmayi Arun, Paper-Thin Safeguards and Mass Surveillance in India, 26 NAT'L L. SCH. INDIA REV. (2014).
[107] Jhalak M. Kakkar et al., The Surveillance Law Landscape in India and the Impact of Puttaswamy (Nat'l L. Univ. Delhi 2023).

UN Special Rapporteur had defined mass surveillance as "when states with high levels of Internet penetration can gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites."[108] According to the report, all of this is feasible in a "mass surveillance" system without any prior suspicions about a particular person or group. The communications of every Internet user are potentially open for inspection by intelligence and law enforcement agencies in the States concerned. [109]

Mass surveillance is considered a global issue, and some people say that the day is not far when states will be called GEOINT Singularity, in which artificial intelligence systems will monitor everything on earth. Many human rights groups and other concerned authorities have started creating awareness about the harms of expanding surveillance. It is a massive problem for normal citizens of the country because they can be denied some essential services if they refuse to give their personal information, and also face prosecution if they do not comply with the rules. The real-world implications of such surveillance driven governance are already evident. For example, the state directly or indirectly controls all internet access in China. China is one of those countries on the track to becoming a surveillance state. The Chinese government is part of an active system of mass surveillance. The Great Firewall of China is China's mass surveillance system that employs Deep Packet Inspection (DPI) technology to monitor and deny access based on keyword detection[110]. Alarmingly, similar trends are observable beyond China. Recently, India bagged a couple of top ranks in Forbes list of the most surveilled cities in the world where Delhi stood at rank one with about 1,826.6 cameras per square mile beating Chinese cities like Beijing, Wuhan, Xiamen, and London etc., Chennai at rank three with 609.9 cameras per square miles and Mumbai at rank 18 with 157.4 cameras per square miles. The Delhi government has restarted phase 2 of its CCTV project to install 140,000 CCTVs.[111]

[108] U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014).
[109] Arghish Akolkar, Government Surveillance Against the Right to Privacy in Matters of Cyberspace in India, ELEC. J. SOC. & STRATEGIC STUD., Vol. 5, Issue 1, 2024
[110] Harsh Bansala, Road to Become a Surveillance State, U.S. CORPUS L.J., Sept.–Nov. 2021,
[111] Kamesh Shekar & Shefali Mehta, The State of Surveillance in India: National Security at the Cost of Privacy?, Observer Res. Found. (July 4, 2023), https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india.

4.3 State surveillance in India

Surveillance in India has its foundations deeply embedded in the colonial legacy of control and governance. During the 1800s, the British colonial government introduced the telegraph as a powerful communication tool, with Governor-General Lord Dalhousie initiating the first line between Calcutta and Diamond Harbour in 1851. For the colonial state, the telegraph was a technological advancement and an "engine of power" used to assert political and military dominance. Though pre-dating colonial rule, the British restructured and standardized the postal system to create a unified and formalized communication mechanism across provinces and presidencies. Crucially, the legislative framework that regulated the postal and telegraph networks was in line with British law, which granted the Secretary of State the authority to conduct surveillance through the royal prerogative. Even though monitoring was not explicitly permitted by British law, it was not considered unlawful. Therefore, government interception was allowed to take place without clear legal restrictions. Surveillance over telegrams and telephonic conversations emerged through broad interpretations of powers previously practiced over letters, but lacked any formal statutory basis. Though extensively used, these powers remained secrecy, with warrant processes hidden from public scrutiny until the Birkett Committee inquiry in 1957 exposed the practice[112].

In British India, however, surveillance powers were more explicitly codified through statutes such as the Indian Telegraph Act, 1885 (ITA)[113] and the Indian Post Office Act, 1898 (IPOA)[114], which granted the colonial government vast authority to intercept, detain, withhold, or disclose messages on the vague grounds of public emergency or public safety. Sections 5 of the ITA 1885[115] and 25 and 26 of the IPOA 1898[116] became powerful tools of colonial surveillance. These powers were employed to curb anti-colonial mobilisation by monitoring and censoring telegrams, letters, and printed materials considered seditious or dangerous. Freedom fighters and revolutionaries, including Mahatma Gandhi, Jawaharlal Nehru, Subhash Chandra Bose, and M.N. Roy, were placed under intense surveillance. Communications of organizations like the

[112] P. Arun, Regressive and Authoritarian: Surveillance Powers in the Telecommunications Act 2023 and Post Office Act 2023, 9 Indian L. Rev. 1 (2024).
[113] The Indian Telegraph Act, 1885
[114] The Indian Post Office Act, 1898
[115] Indian Telegraph Act, § 5, 1885
[116] Indian Post Office Act, § 25, 1898

Hindustan Ghadar Party, the League against Imperialism, and the Communist International were routinely intercepted. The suppression of dissent through surveillance also extended to foreign correspondents. For instance, telegrams sent by Mira Behn to international supporters of the freedom movement, including British MP Tom Williams and French author Romain Rolland, were detained by colonial authorities. These instances reflect how the colonial state weaponize communications technology to suppress political opposition and maintain control over the population.

In his writings, Jawaharlal Nehru expressed the psychological toll of being under constant surveillance, describing it as oppressive and invasive of personal freedom. The colonial surveillance regime was characterized by four key features: complete executive discretion with no external oversight, the ability to amend procedural rules internally, absolute secrecy in the exercise of powers, and intelligence gathering through intercepted communications. These features facilitated authoritarian governance during colonial rule and left a lasting imprint on the Indian surveillance framework after independence. While the makers of the Indian Constitution considered incorporating protections against state intrusion, such as secrecy of correspondence and safeguards against unreasonable searches, these proposals were ultimately dropped due to concerns that such provisions might obstruct investigations and prosecutions in independent India[117].After independence in 1947, the Indian state kept its surveillance powers from the colonial era under the Indian Telegraph Act, 1885 and the Indian Post Office Act, 1898 .

In the following decades, newspapers like Swadhinata routinely placed their postal communications under watch. Efforts to reform these laws gained momentum in the 1970s. The 1972 amendment to Section 5 of the ITA, 1885[118] was intended to align with Article 19(2) [119]of the Constitution. In order to conform to Article 19(2) of the Constitution, Section 5 of the ITA was amended in 1972. It did not, however, define important concepts like "public emergency" and "public safety," which remained ambiguous and prone to abuse. The continuation of colonial regulations was sharply condemned by lawmakers like Sasankasekhar Sanyal and L.K. Advani, who contended

[117] P. Arun, Supra Note 112
[118] Indian Telegraph Act, § 5, 1885
[119] India Const. art. 19, cl. 2.

that such rules had no place in a democratic republic and were intended to stifle free expression and the press during British administration. In the 1980s, private members like Bhai Mahavir and Vaiko introduced bills in Parliament to repeal Section 5 of Indian Telegraph Act, 1885, labelling it "reprehensible," "archaic," and a product of colonial hangover. Nevertheless, these reform efforts failed to gather sufficient political will.[120]

Judicial scrutiny of surveillance practices increased in the 1990s. In a landmark 1994 judgment, the Bombay High Court addressed the misuse of Section 26 of the IPOA 1893 after the CPI (Maoist) Maharashtra Unit complained about unauthorized interception of its postal articles. The Court mandated that reasons must be recorded before exercising such powers, even though the statute itself did not require it, declaring the absence of such reasoning to be an illegal exercise of power. This marked a minimal but crucial safeguard against arbitrary state action.

In the landmark case of People's Union for Civil Liberties v. Union of India (1996)[121], the Supreme Court addressed widespread phone tapping in response to an article exposing illegal interceptions. The Court ordered the government to create regulations to control interceptions after ruling that Section 5 of the ITA 1885 lacked procedural protections. In the absence of such regulations, the Court established temporary safeguards, including creating a review committee that is likewise led by bureaucrats and limiting the authorization of interception to a specific class of senior officials. Notably, the Court kept oversight within the executive branch by not requiring court approval for such surveillance. These directions were subsequently codified in Rule 419-A of the Indian Telegraph Rules, 1951. In recent years, these powers have continued and further grown under the pretence of technical advancement and national security. The institutionalization of mass surveillance systems and malware like Pegasus highlight the increasing concentration of state monitoring powers. This continuity of colonial era surveillance norms into the digital age has laid the groundwork for a more technologically sophisticated and automated surveillance regime. With the emergence of India's contemporary surveillance infrastructure, which includes integrated intelligence networks, dragnet interception systems, and facial

[120] P. Arun, Supra Note 112
[121] People's Union for Civil Liberties v. Union of India, A.I.R. 1997 S.C. 568

recognition technology, analog monitoring has given way to data-driven profiling and predictive policing. [122]

4.3.1 Pegasus Spyware Controversy

The Pegasus spyware incident represents a particularly unsettling development in the state's monitoring capabilities in line with this trend of expanded surveillance authorities. Pegasus is an advanced spyware program created by the Israeli cyber-arms company NSO Group that can infiltrate smartphones and provide unauthorized users access to calls, messages, location information, camera, and microphone features without the user's awareness. Pegasus, which was first identified in 2016 when it targeted the phone of Emirati human rights activist Ahmed Mansoor, is a Trojan Horse virus that uses cutting-edge "zero-link" technology, which takes advantage of flaws in a smartphone's operating system without the target having to do anything, like click a link[123]. The potential for misuse is greatly increased by this feature, which also gets around even the strong encryption provided by messaging apps like Telegram and WhatsApp. In order to secretly capture the environment, the spyware may also remotely activate microphones and cameras and gather passwords and browsing history.

The extent of Pegasus's abuse was made clear on a global scale in July 2021 when a group of international media sites disclosed that about 50,000 phone numbers, including those of journalists, activists, political figures, and human rights advocates, were being monitored. According to reports, these figures were given to Amnesty International and the Paris-based media group Forbidden Stories, which sparked a thorough inquiry known as the Pegasus Project. It was verified that the spyware was used to spy on at least 180 journalists from 20 different nations and well-known international media organizations, including CNN, Al Jazeera, and The New York Times[124].

In India the particular situation drew attention as reports indicated the surveillance of popular journalists, political figures, and activists, raising serious questions about governmental accountability and infringement of fundamental rights. The Supreme

[122] Mohd Faiz Khan , Supra Note 101
[123] Soujaatyaa Roy, The Impact of the Recent Pegasus Spyware Controversy on the Right to Privacy in India, 6 Int'l J.L. Mgmt. & Human. 1060 (2023).
[124] Id.

Court of India established an investigative commission headed by retired Justice RV Raveendran to look into these claims after this matter sparked intense discussion and judicial action. The findings unquestionably demonstrated the seriousness of possible privacy infringement inherent in sophisticated malware, even though the committee's examination of a few devices could not confirm Pegasus's presence on all phones[125].

This development directly squarely challenges the fundamental right to privacy, which was established in K.S. Puttaswamy v. Union of India (2017)[126], where the Supreme Court explicitly recognized privacy as integral to Article 21 of the Constitution. Thus, the Pegasus incident highlights a critical conflict between the protection of constitutional liberties and claims of national security, proposing more robust legal protections and increased openness in oversight processes to obviate excessive government encroachment into individuals' private lives[127].

4.4 Surveillance Schemes in India

The development and use of surveillance tools in India has followed a similar path, with an increase in the deployment of new age surveillance technology such as dragnet systems for electronic surveillance, facial recognition, and the use of data analytics and profiling on individuals. India's modern surveillance programs such as the Central Monitoring System (CMS), the National Intelligence Grid (NATGRID), and Network Traffic Analysis (NETRA) allow for the automation of interception, the facilitating of data sharing for the creation of an integrated intelligence database, and the wholesale (or dragnet) collection of electronic communications to identify threats.[128]While the CMS and NETRA involve primary data collection, programs such as NATGRID, the Crime and Criminal Tracking Network System (CCTNS), and the use of facial recognition technology on CCTV feeds are aimed at centralising and streamlining existing databases of information on individuals.

CCTNS: The Ministry of Home Affairs conceptualized the Crime and Criminal Tracking Network Systems (CCTNS). The CCTNS aims to make it easier for police to

[125] Id.
[126] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1
[127] Id.
[128] Jhalak M. Kakkar et al., The Surveillance Law Landscape in India and the Impact of Puttaswamy (Nat'l L. Univ. Delhi 2023).

gather, save, retrieve, analyse, transfer, and share data and information and enable police to communicate with Central Police Organizations and State Headquarters. Early in January 2013, the CCTNS was publicly introduced in New Delhi. The goal of this project is to provide a comprehensive and integrated system for efficient law enforcement and the exchange of crime and criminal data across 14,000 police stations located throughout India's 35 states and Union Territories. The CCTNS was implemented as part of the national e-governance program and is a component of the police force's modernization effort. CCTNS seeks to develop a complete and integrated system In order to improve the effectiveness and efficiency of police at all levels, especially at the Police Station level, through the adoption of principles of e-governance and the establishing a state wide networked infrastructure to support the development of a cutting-edge tracking system centred on "investigation of crime and detection of criminals" in real-time, which is essential given the current internal security situation. This system improves the function of the police in various other areas, such as Law and Order, Traffic Management, etc.[129]

CMS: Central Monitoring System (CMS) makes use of strong algorithms that can crawl through data to find users and patterns in intrusive ways[130]. A significant change in India's surveillance structure is represented by the CMS, which replaces decentralized, targeted monitoring with centralized, automated mass surveillance. Previously, each Telecom Service Provider (TSP) was required to have Lawful Interception Systems, where interception requests were routed through designated nodal officers. With CMS, however, Interception Store & Forward (ISF) servers are integrated with existing systems and automatically transmit intercepted data to Regional Monitoring Centres (RMCs), which are connected to a centralized CMS hub[131]. This eliminates the need for TSP involvement, significantly reducing oversight. With CMS in place, the government will be able to listen and record phone conversations, read emails and text messages, keep an eye on posts on Facebook, Twitter, or LinkedIn, and track Google searches. In essence, the government will be

[129] Maria Xynou & Elonnai Hickok, Security, Surveillance and Data Sharing Schemes and Bodies in India

[130] Addison Litton, The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression, 14 WASH. U. GLOB. STUD. L. REV.2015

[131] Arghish Akolkar, Government Surveillance Against the Right to Privacy in Matters of Cyberspace in India, 5 Elec. J. Soc. & Strategic Stud. 38 (2024)

monitoring all electronic communications. Emails that are only partially composed and stored in draft files are susceptible to government interference. CMS will also allow the government to deploy location-based GPS monitoring to follow a person's travels. With CMS's assistance, the government will be able to create user personal dossiers by gathering personal data that matches the target numbers provided to those individuals. The Central Board of Direct Taxes (CBDT), the Enforcement Directorate (ED), the National Intelligence Agency (NIA), the Central Bureau of Investigation (CBI), the Research and Analysis Wing (R&AW), the Central Bureau of Investigation (CBI), and the Narcotics Control Bureau are among the agencies that are approved for this scheme.

NETRA: The Indian Government has developed and operationalized the Network Traffic Analysis (NETRA) system, which is reportedly capable of real-time monitoring and detection of suspicious "keywords" and "keyphrases" across social media platforms, emails, blogs, tweets, instant messaging services, and various other forms of internet communication content. It has also been reported that the Ministry of Home Affairs is finalising the NETRA system, which will also likely be capable of capturing any dubious voice traffic through online communications. This system is possibly going to be carried out with the purpose of tackling crime and terrorism in India. The (CAIR) Centre for Artificial Intelligence and Robotics, a lab under the Defence Research and Development Organization (DRDO), is the developer of the NETRA system. The deployment strategy of NETRA was recently discussed between an inter-ministerial group comprising of officials of the Cabinet Secretariat, Home Ministry, DRDO, CAIR, Intelligence Bureau, Centre for Development of Telematics (C-DOT) and Computer Emergency Response Team (CERT-In). This interministerial panel examined NETRA's deployment strategy as well as a plan for handling computer security events, monitoring system vulnerabilities, and encouraging good IT security practices throughout India. [132]

NATGRID: The government established the National Intelligence Grid (NATGRID), an integrated intelligence grid following the Mumbai attack in 2008, to create a framework for strengthening and monitoring India's counterterrorism operations. The National is proposed to connect the databases of several Indian government ministries

[132] Harsh Bansala , Supra Note 110

and departments to gather comprehensive intelligence patterns that intelligence agencies can easily access. The first phase of NATGRID, which is regarded as a data linking and mining initiative, would have included "real-time linking" of data amongst different agencies.[133] It seeks to gather sensitive information from databases of authorities like the police, banks, tax, and telecom to track any terror suspect and incident. This initiative will enable real-time profiling of individuals via gathering, combining, and analyzing their metadata, which may reveal various kinds of information.

Similarly, we have seen the proliferation of digital IDs in India as well. From Aadhaar (a biometric and digital ID) to the National Health Stack, the National E-Transport Project, and DigiYatra , Arogya sethu the government has been increasingly collecting sensitive personal data about its citizens and creating more detailed profiles. This highlights the need for effective data protection legislation.

Aarogya Setu: It is launched in April to obtain location details of users and the persons with whom they come in contact. The App seeks to collect personal details such as name, gender, health status, travel history and even obtains the user's contact list to determine the risk status of users. This information is intended to help health authorities manage infection outbreaks. With over 75 million downloads, Aarogya Setu quickly became one of the fastest downloaded applications. The App was made "mandatory" for certain public sector employees who were forced to download the application, while in some cities people were penalized for not having the application.[134]

DigiYatra: The Ministry of Civil Aviation introduced DigiYatra, an opt-in service at Indian airports, in 2017 with the goal of making air travel "seamless, contact-less, hassle-free, and paperless" for every traveller. By replacing traditional boarding cards with facial recognition technology (FRT) and Aadhaar-linked credentials for authentication, the service allows travellers to be processed digitally at airports. The DigiYatra Biometric Boarding System (DYBBS) Policy is the framework which guide

[133] Arghish Akolkar, Government Surveillance Against the Right to Privacy in Matters of Cyberspace in India, ELEC. J. SOC. & STRATEGIC STUD., Vol. 5, Issue 1, 2024

[134] Mira Swaminathan & Arindrajit Basu, Surveillance and Data Protection: Threats to Privacy and Digital Security *(*2020) https://cis-india.org/internet-governance/blog/india-digital-freedoms-5-surveillance.

the implementation and regulation of the DigiYatra program. Despite being promoted as secure and optional, the DYBBS Policy and DigiYatra's Privacy Guidelines raise serious privacy and legal issues. The amount and kind of data gathered is one of the most urgent problems. According to DigiYatra's Privacy Policy, the program gathers a broad spectrum of personal data, including—but not limited to—identity and contact details, biometric data, business information, passwords, images, and video recordings. This data is collected through mobile applications, and e-gates at airports. While passengers are asked to give consent, the policy lacks transparency regarding the exact purposes for data collection, often stating vaguely that the information may be used for "product improvement," "customer surveys," and "processing user requests."[135]

Biometrics: Biometrics is the science and technology of measuring and statistically analysing biological data. In information technology, biometrics refers to technologies for measuring and analysing human body characteristics. Biometric markers are the most unique types of personal information, since they are specific to every individual. Fingerprinting for example, is perhaps the oldest and most commonly used type of biometric data. However, technological advances has enabled surveillance companies to harvest and track newer forms of biometric data as well. Some of the newer biometric identifiers are facial/retinal recognition, voice recognition, skin reflection and thermo grams. Various types of biometric surveillance are becoming increasingly common areas with large human influx, such as shopping malls, stadiums, banks, airports and transportation. The granularity of biometric data, as well as the ease with which they can be stored and use for long periods of time, have led to their rise in popularity, especially with high population density areas[136]. Biometrics involves comparing a previously captured, unique characteristic of a person to a new sample provided by the person. The biometric information is used to identification or verification of a persons to find out whether they are who they claim to be. This process can mean an attack on one's privacy when the collection takes place without consent or permission and without transparency about the purpose for which this data is used. While these programs are essentially welfare schemes aimed at improving electronic governance,

[135] Disha Verma, Digi Yatra: A Service or Surveillance?, The India Forum, (Feb. 8, 2024), https://www.theindiaforum.in/article/digi-yatra-service-or-surveillance.
[136] Akin Unver, Politics of Digital Surveillance, National Security and Privacy (Ctr. for Econ. & Foreign Pol'y Stud. 2018).

insofar as they increase governmental access to personal data, they present surveillance risks. These schemes also raise data access and purpose limitation concerns vis-a-vis the personal data of individuals[137].

National ID: Due to the lack of proper ID, India faces the problem of tracking illegal immigrants, counterfeit identification, bogus voting and inaccurate voting rosters during each election. Hence, the government has argued, the introduction of smart card-based National ID documents is natural in such an environment. Every identity system is made up of a support register containing personal information parallel to that on the ID card. When this information is maintained on a central database, the ID number acts as a common identifier for multiple government agencies. The risks that this poses for individual privacy are monumental. Centralized information is centralized power. A national identifier contained in an ID card enables disparate information about a person scattered in different databanks to be easily linked and analysed through data mining techniques. This would allow the entries in one set of data to influence other, unrelated parameters. Moreover, multiple agency access to sensitive data (or multiple-use of the ID card) greatly increases the potential for misuse of personal information (by 'snooping', social sorting and profiling), either through corrupt disclosure, or lapses in security[138].

Adhaar Card: In 2009, the UPA Government introduced the Aadhaar project. For a variety of uses in India, the Aadhaar card has become the dominant form of identification over time. The total number of Aadhaar cards issued by the end of 2019 exceeded 1.25 billion. Since its launch, the Aadhaar-based authentication services have been utilized nearly 37,000 times. Under the terms of the Aadhaar Act, 2016[139], the Indian government established the Unique Identification Authority of India (UIDAI) on July, 2016, to carry out the Aadhaar project. It is the biggest biometric identifying system in the world. The programme envisages a 12-digital UID to collect demographic and biometric data which includes iris scans, facial pictures, and fingerprints that can

[137] Jan Holvast, History of Privacy, in IFIP Advances in Information and Communication Technology 13 (2009).
[138] Sheetal Asrani-Dann, The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National ID Cards in India, 47 J. INDIAN L. INST. 53 (2005)
[139] Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

be linked to access various services like food rations, subsidies, pensions, and other financial services.

It promoted biometric verification, authentication, and identification as an optional option, which is benefiting the general population seeking food subsidies andwelfare schemes. Aadhaar was initially developed to make it easier to provide social assistance, but in recent times, its implementation has increased exponentially. 2017, the government had mandated its use for various programmes and schemes, including for tax compliance, bank account usage, educational scholarship awards, public Wi-Fi access, pension payments, and maternity benefits. This increased digital interconnectivity, the likelihood of other entities accessing identifying information too increases[140]

4.5 Privacy Vis a Vis Surveillance

The tension between privacy and state surveillance has become one of the most pressing constitutional debates of the 21st century, especially after the 2013 Edward Snowden disclosures. These revelations uncovered the vast, global surveillance architecture maintained by American and British intelligence agencies through programs like PRISM and TEMPORA, which were used to monitor not only foreign communications but also domestic populations[141]. The global shockwaves of these disclosures prompted countries, including India, to examine their own surveillance regimes. In India, the issue gained legal prominence when the government defended the Aadhaar scheme by asserting that the Indian Constitution did not guarantee a fundamental right to privacy. This argument, rooted in outdated Supreme Court rulings such as MP Sharma v. Satish Chandra[142] and Kharak Singh v. State of UP[143], was ultimately rejected in the landmark 2017 judgment of Justice K.S. Puttaswamy v. Union of India[144].

[140] Kathryn Henne, Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India, RUSS. SOCIO. REV. (2019).
[141] Gautam Bhatia, State Surveillance and the Right to Privacy in India: A Constitutional Biography, 26 NAT'LL.SCH. INDIA REV. 127 (2014)
[142] M.P. Sharma v. Satish Chandra, 1954 S.C.R. 1077 .
[143] Kharak Singh v. State of U.P., (1964) 1 S.C.R. 332.
[144] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

In Puttaswamy, a nine-judge bench of the Supreme Court unanimously held that privacy is a fundamental right intrinsic to life and personal liberty under Article 21 of the Indian Constitution. The Court explicitly overruled earlier decisions that denied the constitutional protection of privacy and laid down an analytical framework for assessing state actions that infringe on privacy, namely the proportionality test. This test requires any restriction on privacy to be backed by law, serve a legitimate aim, be necessary and proportionate to that aim, and be accompanied by procedural safeguards. Importantly, the Court also recognised the broader harms of surveillance, including its chilling effect on free speech, its impact on psychological autonomy, and its role in reinforcing the power imbalance between the state and its citizens[145].

This judgment emphasized that surveillance, even without actual misuse, creates an environment of self-censorship and fear. Drawing on Justice Subba Rao's dissent in Kharak Singh[146], which described the psychological constraints caused by being watched, the Court acknowledged that the very existence of a surveillance apparatus can stifle individual freedoms. Knowing that one's communications, movements, or associations might be monitored by the state alters behaviour, discourages dissent, and restricts the free development of thought essential elements of democratic participation[147].

Moreover, the Court highlighted the dangers of secret surveillance where individuals are unaware that they are being monitored which denies them the opportunity to seek redress or challenge state overreach[148]. This concern is particularly acute in India, where several intelligence agencies, such as the Intelligence Bureau (IB), the Research and Analysis Wing (R&AW), and the Central Bureau of Investigation (CBI), function without clear statutory frameworks or independent oversight. As a result, citizens are vulnerable to unchecked surveillance with little accountability or transparency[149].

[145] Id.
[146] Kharak Singh v. State of U.P., (1964) 1 S.C.R. 332.
[147] Apar Gupta, The Supreme Court's Right to Privacy Decision: Reading Between the Lines, 12 Indian J. Const. L. 55, 67–69 (2018)
[148] Gautam Bhatia, State Surveillance and the Right to Privacy in India: A Constitutional Biography, 26 Nat'l L. Sch. India Rev. 127, 134–136 (2014)
[149] Ujwala Uppaluri, The Privacy Hearings: Some Notes on Supreme Court Practice, Law and Other Things (July 22, 2017)

In the digital age, these concerns are amplified. The capacity of the state to collect, analyse, and store personal data has grown exponentially through GPS tracking, facial recognition, metadata analysis, and algorithmic profiling. As noted above technology has made surveillance cheaper, easier, and far more invasive than in the past, threatening to erode the practical and constitutional protections that once shielded individuals from arbitrary state intrusion. The Court recognized that in a constitutional democracy, the right to privacy is vital not only for individual dignity but also for the protection of marginalized communities and the maintenance of democratic discourse.[150]

While Puttaswamy rightly affirms the fundamental importance of privacy in a constitutional democracy, it also acknowledges that the right is not absolute and may be justifiably restricted under specific constitutional parameters. This recognition opens the door to a nuanced understanding of justification for surveillance, wherein the state may invoke compelling interests such as national security, efficient governance, and crime prevention. Surveillance is often defended as essential to national security, particularly in addressing cross-border terrorism, internal insurgencies, and cyber threats, where early detection and prevention are vital to safeguarding sovereignty and public safety. It is also positioned as a means to enhance administrative efficiency facilitating better service delivery, monitoring welfare distribution, and reducing corruption through digital integration. Additionally, surveillance supports law enforcement in preventing, investigating, and solving crimes, especially in densely populated or high-risk areas. However, for such surveillance measures to align with constitutional values, they must be lawful, necessary, proportionate, and accompanied by strong safeguards and oversight mechanisms that prevent misuse and uphold democratic freedoms.

4.6 Legal Justification of Surveillance

Monitoring by the state is not always illegal. Governments have justifiable justifications for conducting surveillance that are not based on a desire to restrict personal liberties and impose political repression.

[150] Jhalak M. Kakkar et al., The Surveillance Law Landscape in India and the Impact of Puttaswamy (Nat'l L. Univ. Delhi 2023).

1. National Security

Following high-profile terrorist attacks like 9/11 in the US and 26/11 in India, the government contends that security-based surveillance is an essential tool for maintaining national security. The finest illustration of this change is the Central Monitoring System (CMS) in India, which reflects a move away from focused surveillance of known criminals and toward widespread communication interception, supported by the necessity of identifying possible dangers before they become real. Technological advancements, such as NATGRID, NETRA, and AFRS (Automated Facial Recognition System), are framed not merely as options but as necessities in an era of evolving and unpredictable security challenges. The state legitimates surveillance through an appeal to a wider public interest, usually employing a broad and vague category such as "suspicious people" or "persistent protesters" to justify monitoring, so that the state extends its scope beyond the classical criminal suspect. The lack of judicial or legislative scrutiny, along with public fear and a desire to sacrifice privacy for security, serves to encourage the argument that surveillance is a proportionate and even necessary response in the struggle against terrorism and crime. Consequently, security-based surveillance becomes a self-justifying mechanism, enabled by legal ambiguity, technological capacity, and societal consent under perceived threat[151].

There was an exception in In Manohar Lal Sharma v. Union of India,[152] the Supreme Court of India considered petitions seeking an independent probe into allegations that the government had used Pegasus spyware to surveil journalists, activists, and public officials. The Court acceded to the petitioners' request for a judicial investigation, emphasizing that although the scope of judicial review in matters involving national security is admittedly limited, such matters are not beyond the reach of constitutional scrutiny. Crucially, the Court asserted that the State cannot be granted a "free pass" merely by invoking the phrase "national security," cautioning that ″national security cannot be the bugbear that the judiciary shies away from, by virtue of its mere mentioning.[153]″

[151] Sangeeta Mahapatra, Digital Surveillance and the Threat to Civil Liberties in India, GIGA FOCUS ASIA, No. 3 (May 2021)
[152] Manohar Lal Sharma v. Union of India, AIR 2021 SC 5396.
[153] Id.

2. Efficient Governance

Surveillance under governance-by-insight, in India has its core rationale in the quest for administrative effectiveness and universal access to welfare programmes, and at the centre of this stands the project Aadhaar. Initiated in 2009 and subsequently receiving juridical sanction in 2016, Aadhaar was conceived as a tool to make service delivery efficient and cut waste in welfare through the allotment of every citizen a unique biometric identity. Nevertheless, the integration of the system into daily life on the basis of compulsory linking with bank accounts, mobile numbers, ration cards, and pensions has changed its nature from facilitative to coercive, converting informed consent into forced consent. By compiling biometric and demographic information, the state creates a "digital duplicate" of citizens, functionally infusing surveillance into the fabric of day-to-day governance. This transition is rationalized by the state as required for effective governance, but it allows for constant monitoring and profiling of citizens, frequently at the expense of privacy and self - determination. Exclusion of marginalized groups such as those excluded from receiving food rations due to Aadhaar-related mistakes also serves to demonstrate how surveillance-enabled governance can yield structural inequality. Initiatives such as the National Digital Health ID and the move to connect Aadhaar with the National Register of Citizens reflect the potential for surveillance as a tool of control, especially in the event of lack of strong data protection legislation. The state's powers to access and disseminate intimate health and demographic data, even to third parties, are justified on grounds of policy effectiveness but run the risk of breaching fundamental rights. So, surveillance based on governance is justified as a means of modernization and integration, even as it facilitates concentration of power and loss of privacy[154].

3. Prevention of Crime

Crime prevention is most often cited as a real-world and socially desirable reason for state surveillance, especially in the face of increased urbanization, cybercrime, and organized crime networks. The state maintains that surveillance technologies like CCTV networks, predictive policing software, call intercept systems, and crime databases improve its ability to identify, deter, and react to criminal acts in real-time

[154] Id.

and effectively[155]. Real-time tracking of public spaces and online communications is presented as critical for detecting abnormal activity, monitoring known criminals, and reacting to threats before they materialize. For example, surveillance via India's Crime and Criminal Tracking Network Systems (CCTNS) connects thousands of police stations around the country, allowing for the free exchange of information between jurisdictions. Predictive policing technology, likewise, is warranted as analytics driven methods of more effective deployment of police resources, particularly where there is high incidence of crime. In its creation of an atmosphere of all around vigilance, surveillance is also thought to discourage would be culprits, promoting law and order. And since crime is now increasingly going online anything from cyber fraud to online harassment the digital surveillance of internet activity, phone use, and financial transactions is presented as a necessity. The state therefore constructs surveillance not as an invasion, but as a safeguard that protects citizens and maintains public security. And yet the rationale is based on the premise that this kind of surveillance is proportionate, accountable, and properly regulated in law otherwise it could easily descend into overreach, disproportionately targeting already vulnerable communities, and undermining civil liberties in the name of protection[156].

While national security, crime prevention, and governance efficiency are the three dominant pillars upon which the state justifies its growing surveillance apparatus, these justifications must ultimately rest on a foundation of legality, proportionality, and accountability. The legitimacy of any surveillance regime hinges not just on purpose but on whether it is supported by a strong legislative framework that safeguards fundamental rights, provides procedural protections, and facilitates independent monitoring. Globally, even democratic nations with strong legal traditions often fall short in upholding these standards, and the risks are magnified in contexts where data protection laws are weak or absent. As the United Nations' Office of the High Commissioner for Human Rights (OHCHR) has noted, states that lack adequate legislation and oversight mechanisms create conditions ripe for abuse, making surveillance a tool of control rather than security.

[155] Muktesh Chander, E-Surveillance, Academy J., Dec. 2003, at 13
[156] Id.

4.7 Conclusion

Considering the need for surveillance, particularly in light of the circumstances surrounding the Mumbai attack, it would seem illogical to advocate for its complete prohibiting. Protecting national security in the fight against terrorism requires proactive measures. In India, especially in a vast and diverse democracy, the idea that collective security comes before individual liberty has gained acceptance. However, the legal and constitutional aspects of surveillance are still vague and undeveloped[157].

In Justice K.S. Puttaswamy v. Union of India[158], the constitutional guarantee of privacy that states that any governmental intrusion into personal data must follow the standards of legality, necessity, and proportionality is undermined by these shortcomings[159].

Furthermore, the potential of unrestrained state intervention into individual autonomy has increased due to the expansion of mass surveillance systems such as CMS, NETRA, NATGRID, and Aadhaar-linked digital governance—without adequate protections[160]. The frequent use of ambiguous terms like "public order" and "national security" plus the lack of accountability processes result in a monitoring infrastructure that is susceptible to overreach and chronic abuse.

It is therefore imperative to analyse the surveillance framework in India to ensure a balance between national security and the protection of fundamental rights.

[157] Usha Ramanathan, State Surveillance and the Right to Privacy in India, 50(22) Econ. & Pol. Wkly. 12 (2015).
[158] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1
[159] Sandeep Bhushan, Paper-Thin Safeguards and Mass Surveillance in India, 50(22) Econ. & Pol. Wkly. 10 (2015)
[160] Usha,Supra Note 157

CHAPTER 5

LEGAL FRAMEWORKS AND REGULATORY GAPS: AN ANALYTICAL OVERVIEW

5.1 Introduction

In the information age, state surveillance has redefined traditional notions of individual freedom, responsibility, and governance. The state can now monitor, collect, and analyze vast amounts of personal information with unprecedented speed and precision due to technological advances. The right of privacy, being an integral element of human dignity and democratic society, faces serious danger due to monitoring, even if it can be defended on grounds of public order, national security, or administrative efficiency[161].

The validity of surveillance in constitutional democracies relies on independent surveillance, clearly formulated legal limits, and procedural safeguards. But the legal framework that regulates surveillance in India remains deeply opaque, executive oriented, and dispersed. The lack of a coherent, rights-based framework has enabled surveillance to flourish in legal and moral grey areas, frequently without serious accountability or judicial oversight. This has spawned an unsettling skew between state authority and personal freedom, triggering fears about the denigration of essential constitutional principles[162].

Given these concerns, it becomes necessary to conduct a critical evaluation of India's surveillance system to ascertain if it is in consonance with the constitutional vision of privacy, procedural justice, and democratic accountability.

[161] Chinmayi Arun, AI and the Right to Privacy in India: Emerging Constitutional Questions, 3 Indian J. Const. L. 111, 115 (2020).
[162] Apar Gupta, India's Surveillance Framework and the Need for Reform, 14 NUJS L. Rev. 1, 8–12 (2021)

5.2 Legislative Framework

1. Information Technology Act, 2000[163]

This Act is one of the primary laws regulating interception, monitoring, decryption, and collection of digital communications and information. The Act is grounded on the United Nations Commission on International Trade Law (UNCITRAL). In the year 1996 the UNCITRAL adopted the Model Law on Electronic commerce .India was also a signatory to this and hence was expected to introduce laws as per the Model Law. The Information Technology Bill was drafted in 1998 and subsequently reviewed by a Parliamentary Standing Committee, which recommended certain modifications. The Ministry of Information Technology incorporated some of these suggestions, and the revised bill was approved by the Union Cabinet and passed by both houses of Parliament. After receiving the President's assent on June 9, 2000, the Information Technology Act, 2000, came into force on October 17, 2000.

Section 69 of the Information Technology (IT) Act, 2000, deals with the power to issue directions for interception, monitoring or decryption of any information through any computer resource. This Section stipulates that the central government or the state government or the officers specially authorized by them may, if satisfied that it is necessary or expedient to do so, by order, direct any agency of the appropriate government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received, or stored in any computer resource. For this, the reasons shall be recorded in writing[164].

According to section 69(2) the exercise of the powers under Section 69(1) can only be done in the interest of the sovereignty or integrity of India, security of the State, friendly relations with the foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. The procedure and safeguards for such interception, monitoring or decryption shall be such as may be prescribed[165].

[163] The Information Technology Act, 2000
[164] Id. § 69(1)
[165] Id. § 69(2).

Section 69(3) of the Information Technology Act, 2000, mandates that any subscriber, intermediary, or person in charge of a computer resource must provide all facilities and technical assistance to authorized government agencies for intercepting, monitoring, or decrypting information when legally directed. This includes granting access to the computer resource, facilitating interception or decryption, and supplying stored information. Non-compliance with such directives constitutes a criminal offense under Section 69(4), punishable by imprisonment for up to seven years and a fine[166].

Section 69A of the Information Technology Act, 2000, empowers the Central Government or its specially authorized officers to direct any government agency or intermediary to block public access to information hosted on computer resources. Such directives can be issued when deemed necessary or expedient in the interest of India's sovereignty, defense, state security, friendly relations with foreign states, public order, or for preventing incitement to the commission of any cognizable offense. The reasons for such actions must be recorded in writing. The procedure and safeguards for blocking public access are prescribed under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. Non-compliance with these directives by intermediaries can result in imprisonment for up to seven years and a fine[167].

Section 69-B deals with the power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. According to the Section, the Central Government by notification in the Official Gazette, may authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. The Central Government may do so in order to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer containment in the country. ("Computer contaminant" refers to any set of computer instructions designed to either (a) modify, destroy, record, or transmit data or programs residing within a computer,

[166] Id. § 69(3)–(4).
[167] Id. § 69A

computer system, or computer network, or (b) usurp, by any means, the normal operation of the computer, computer system, or computer network.) [168]

The intermediary or any person in-charge of the computer resource shall provide technical assistance and extend all facilities to the authorized agency when called to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

For monitoring and collecting traffic data or information, the procedure and safeguards shall be such as may be prescribed. If an intermediary knowingly or intentionally refuses to comply with the provisions outlined in Sub-section (2), which requires them to assist authorized government agencies in monitoring and collecting traffic data, they can face imprisonment for up to three years and may also be subject to a fine.

According to the provisions of this act, it is permissible to intercept all electronic transmissions of data Thus, these Sections delineate the powers of the central government to interception, monitoring and decryption of the data and information contained in the computer resource.

2. The Information Technology (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009[169]

The IT Rules, 2009 were introduced to establish a system of checks and balances and to ensure a structured and appropriate procedure for the interception of information. These rules have been notified under clause (y) of sub-section (2) of Section 87, in conjunction with sub-section (2) of Section 69 of the Information Technology Act, 2000.

Rule 3 is an elaborated provision which mandates Interception, monitoring, or decryption of any information generated, transmitted, received, or stored in any computer resource under section 69(2) of the Act can only be carried out by an order

[168] Id. § 69B
[169] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

from the competent authority. In unavoidable circumstances, an officer not below the rank of Joint Secretary to the Government of India, authorized by the competent authority, may issue the order[170].

In emergencies, such as remote areas where prior directions are infeasible or operational reasons preventing prior directions, interception may be done with the approval of the head or second senior-most officer of the security agency at the Central level and an officer not below the rank of Inspector General of Police or equivalent at the State/Union territory level. The officer approving the interception must inform the competent authority in writing within three working days and obtain approval within seven working days. If approval is not obtained within this period, the interception will cease, and no further interception may occur without prior approval[171].

According to Rule 4, the competent authority has the power to authorize a government agency to intercept, monitor, or decrypt information in any computer resource, but only for the specific purposes outlined in Section 69(1) of the Act.[172]

Rule 8 mandates that before issuing any direction under Rule 3, the competent authority must first assess whether the required information can be obtained through other reasonable means. A direction for interception, monitoring, or decryption may only be issued if no alternative methods are feasible. This requirement acts as a safeguard, limiting the use of Rule 3 to situations where other means of information acquisition are genuinely unavailable[173]

Rule 11 provides that the direction for interception or monitoring or decryption shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty day.[174]

[170] Id. r. 3.
[171] Id.
[172] Id. r. 4.
[173] Id. r. 8.
[174] Id. r. 11

Rule 22 mandates that all records, including electronic records, related to directions for interception, monitoring, or decryption of information, as well as the resultant data, must be destroyed by the security agency within six months.[175]

3. Telecommunication Act, 2023[176]

The Telecommunications Act of 2023 is key piece of legislation in India replaces two old laws: the Indian Telegraph Act of 1885, the Wireless Telegraphy Act of 1933. This new Act marks a big step forward in modernizing the country's telecom regulations.

Section 20 of the Telecommunications Act, 2023 empowers the Central Government, a State Government, or any officer specially authorised in this behalf, upon the occurrence of any public emergency or in the interest of public safety, to take necessary measures by notification[177]. These may include taking temporary possession of any telecommunication service or network from an authorised entity or ensuring priority routing of messages for users involved in emergency response. Further, in the interest of the sovereignty and integrity of India, defence and security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of an offence, the competent authority may, by order and for reasons recorded in writing and subject to prescribed procedure and safeguards, direct the interception, detention, disclosure, or non-transmission of any message in intelligible format. However, press messages of accredited correspondents shall not be intercepted or detained unless prohibited under such order[178].

Section 21 provides that the Central Government may, if satisfied that it is necessary or expedient so to do in the interest of national security, friendly relations with foreign States, or in the event of war, by notification, take such measures as may be required[179]. These include issuing directions regarding the use of telecommunication services, equipment, networks, and identifiers; prescribing standards for manufacture, import, and distribution of telecom equipment; mandating procurement from trusted sources; prohibiting or suspending use of specified telecom equipment or services from notified

[175] Id. r. 22
[176] The Telecommunication Act, 2023
[177] Id. § 20(1).
[178] Id. § 20(2).
[179] Id. § 21(1).

persons or countries; or taking over control and management of telecom services or networks, either wholly or in part, as the circumstances may necessitate[180].

4. Digital Personal Data Protection Act, 2023[181]

In India, the Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark law pertaining to privacy and data protection. By striking balance between the advantages of technology advancement and the necessity of protecting individual privacy rights, this significant law aims to create a new paradigm[182].

According to Section 7(c) of the Act, *2023 "A Data Fiduciary may process personal data of a Data Principal... for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State."*

This clause permits the government or its agencies to collect, use, and process the personal data of individuals without their consent when carrying out any legal function assigned under existing laws in India or when such processing is deemed necessary in the national interest, including for protecting the sovereignty and integrity of India, ensuring State security, or preventing activities that may pose a threat to the nation[183].

Section 17(2)(a) of the Digital Personal Data Protection Act, 2023 empowers the Central Government to exempt any of its agencies from the application of the Act by issuing a notification, on the grounds such as the sovereignty and integrity of India, security of the State, public order, or foreign relations[184]. This means that such agencies can collect, process, and share personal data without adhering to the Act's core safeguards such as consent, purpose limitation, or user rights simply on the basis of executive discretion.

[180] Id. § 21(2).
[181] The Digital Personal Data Protection Act, 2023
[182] Dr. Pradip Kumar Kashyap, Digital Personal Data Protection Act, 2023: A New Light into the Data Protection and Privacy Law in India, 2 ICREP J. INTERDISC. STUD. (2023).
[183] Id. § 7(c).
[184] Id. § 17 (2) (a)

Section 36 of the Act grants the Central Government the authority to require the Data Protection Board, any Data Fiduciary or intermediaries to furnish any information it may request.[185]

5. The Aadhar(Targeted Delivery of Financial and Other Subsidies , Benefits and Services) Act, 2016 [186]

Section 33(2) of the Aadhaar Act introduces an exception to the confidentiality and data-sharing restrictions under Sections 28 and 29, allowing disclosure of identity information or authentication records in the interest of national security. This can only occur pursuant to a direction from an officer not below the rank of Secretary to the Government of India, specifically authorized by the Central Government. Such directions are subject to review by an Oversight Committee, consisting of the Cabinet Secretary and Secretaries of Legal Affairs and IT, and are valid for three months, extendable for another three months after review[187]. This sub-section overrides various provisions, including Section 28(2) (which mandates confidentiality of Aadhaar data), Section 28(5) (which prohibits unauthorized disclosure by UIDAI or its staff), Section 29(1)(b) (which restricts the use of core biometric information to Aadhaar generation and authentication), Section 29(2) (which limits the sharing of identity data), and Section 29(3)(b) (which requires entities to inform individuals about the use of their data).[188] Section 33(2) permits disclosure, use, and sharing of Aadhaar data for national security purposes without individual consent or prior notification[189].

5.3 Gaps in Existing Frameworks

1. IT Act, 2000[190] And IT Rules, 2009[191]

- Lack of Judicial Oversight:

[185] Id. § 36
[186] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[187] Id. § 33(2)
[188] Id. § 28(2), 28(5), 29(1)(b), 29(2), 29(3)(b).
[189] Id. § 33(2).
[190] The Information Technology Act, 2000
[191] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

One of the primary fallacies in the IT Rules 2009[192] is the absence of judicial oversight in the interception process. The authority to issue interception orders lies solely with the executive branch and review by an internal Review Committee. This creates an inherent conflict, as the same organ of the State acts as both the authorising and reviewing authority.

- Vague and Overbroad Grounds:

The grounds on which interception can be authorised under Rule 3 are imprecise and excessively broad. Terms like "public order," "preventing incitement," or "investigating offences" are not clearly defined, leaving them open to subjective interpretation. This vagueness contravenes the principle of legality and fails the test of foreseeability and precision in law. It enables the State to potentially authorise surveillance in a disproportionate and arbitrary manner[193].

- Absence of Procedural Transparency:

The rules do not mandate any form of notification to the person whose data is intercepted, nor do they provide a mechanism for such individuals to contest the interception. While secrecy may be justified in ongoing investigations, the complete denial of a post-facto review or redress for wrongful surveillance violates the principles of natural justice,

- Extended Surveillance Duration (Rule 9)

The rules permit surveillance orders to remain in effect for up to 60 days, with possible extensions to a total of 180 days, all authorized internally by the executive. There is no requirement for a fresh evaluation of the necessity or legality of continued surveillance during this extended period[194]. This allows for long-term, unchecked monitoring of individuals, without any judicial intervention or mandatory periodic reassessment,

[192] Id.
[193] Id. r. 3.
[194] Id. r. 9

raising concerns about function creep, where surveillance becomes a routine rather than exceptional measure.

- Failure to Satisfy Proportionality and Necessity

The Rules do not require that interception be used as a last resort or that it satisfy the test of necessity and proportionality. As laid down in Puttaswamy[195], any restriction on the right to privacy must pass a three-pronged test: legality, proportionality, and procedural safeguards. The Rules fall short on all these counts by failing to ensure that less intrusive means are considered before authorising interception, thereby facilitating excessive state surveillance.

- Over-Reliance on Service Providers Without Accountability

Rule 19 mandates telecom and internet service providers to cooperate fully and maintain secrecy when executing surveillance orders. However, the rules place no liability or safeguards on these providers to ensure the legality of the orders or protect user privacy[196]. This transforms private entities into surveillance agents of the state, often compelled to act without transparency or recourse. The lack of accountability or oversight mechanisms for service providers raises the risk of wrongful interception, violating both the privacy and informational autonomy of users.

- Destruction of intercepted data

Rule 23 of the Information Technology (Interception, Monitoring, and Decryption) Rules, 2009 mandates the destruction of records related to interception, monitoring, or decryption of information within six months of the order being executed. This provision raises concerns over transparency, as it prevents the public from knowing how many decryption or surveillance orders have been issued[197]. It also complicates legal recourse for individuals whose privacy may have been violated, as destroyed records prevent them from proving surveillance in court. This creates a challenge in balancing national security needs with the protection of individual privacy rights.

[195] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1
[196] Rules 2009, Supra note r. 19
[197] Id. r. 23.

2. Telecommunication Act, 2023[198]

- Broad and Vague Grounds for Surveillance

Sections 20(1) and 20(2) allow the Central or State Government or any specially authorised officer to intercept, detain, or prohibit messages, or even take over telecom networks, during a "public emergency**"** or in the "interest of public safety.[199]" These terms are not clearly defined**,** giving authorities wide discretion. This opens the door for subjective interpretation and potential misuse[200]**.**

- Absence of Judicial Oversight

The Act does not mandate prior judicial review or independent oversight, such as through a judge or judicial body. Executive authorities are allowed to authorize surveillance themselves, raising serious questions about checks and balances[201]**.**

- Mandatory Decryption

Section 20(2)(a) of the Telecommunications Act, 2023 empowers the government to intercept and require disclosure of messages in an "intelligible format," thereby undermining end-to-end encryption[202]. This provision effectively obliges platforms to facilitate decryption or retain readable copies of messages, compromising digital security and user privacy. Such measures pose significant concerns regarding the infringement of the right to privacy guaranteed under Article 21 of the Constitution.

- Lack of Specific Procedural

While the TA 2023 formally grants suspension power under section 20(2)(b), it lacks the specific procedures for authorizing and reviewing suspension orders[203].

[198] The Telecommunication Act, 2023
[199] Id. § 20(1).
[200] Id. § 20(2).
[201] Id.
[202] Id. § 20(2)(a)
[203] Id. § 20(2)(b)

3. Digital Personal Data Protection Act, 2023[204]

- Vague and Overbroad Exemptions for the State

Section 7(c) of the Digital Personal Data Protection Act, 2023 allows the State to process personal data without consent for legal functions or in the interest of sovereignty, security, or public order. However, the absence of definitions for terms like "sovereignty," "security," and "public order" leads to ambiguity, enabling broad and potentially arbitrary interpretations that could justify extensive data processing under the guise of national interest[205].

- Blanket Exemption to Government Agencies

Section 17(2)(a) of the Digital Personal Data Protection Act, 2023 empowers the Central Government to exempt any State agency from the provisions of the Act in the interests of sovereignty, national integrity, or State security. This provision is concerning as it permits the executive to unilaterally exempt itself or any agency from fundamental data protection principles without judicial review or independent scrutiny. Consequently, it establishes a parallel framework where the State may engage in surveillance activities without being constrained by privacy safeguards[206].

- Lack of Safeguards Against Misuse

Sec 36 gives the executive wide-ranging power to access data and related information without clearly defined limits, safeguards, or the need to demonstrate necessity or proportionality. The absence of procedural checks or independent oversight raises concerns about potential misuse and intrusion into personal privacy, particularly when exercised alongside other broad exemptions granted under the Act[207].

- Absence of Judicial or Parliamentary Oversight

The Act places exclusive trust in the executive to define and regulate its own surveillance powers, without incorporating any checks or balances. Notably, it lacks

[204] The Digital Personal Data Protection Act, 2023
[205] Id. § 17(c).
[206] Id. § 17(2)(a).
[207] Id. § 36.

provisions for judicial authorisation of surveillance, thereby excluding independent oversight and raising serious concerns about the potential for abuse of power and infringement of individual privacy rights[208].

4. Aadhar Act, 2016[209]

- Lack of Independent Oversight Mechanism

The work of reviewing the orders issued by the government authorities was assigned in the original Act to a three-member Committee of Secretaries of the Central Government. It would have been better if the work of oversight could be assigned to a Parliamentary Committee and the appropriate Court[210]. The involvement of Legislature and the judiciary could have instilled more transparency in the implementation of the Aadhaar project, thereby enhancing the faith and confidence of the people in the whole system

- Broad and Vague Grounds for Data Disclosure

The Act does not define "national security," thereby granting wide discretionary power to the executive. This vagueness creates significant potential for misuse and arbitrary surveillance.[211]

5.4 Conclusion

The analysis of India's surveillance system only shows a framework entrenched in secrecy, overreach, and executive dominance. What is revealed is not a collection of antiquated laws or procedural deficiencies, but a structural neglect of the principles that underlie constitutional democracy. In the lack of effective judicial, legislative, or civil checks surveillance as a practice has gradually shifted from an exception to an administrative norm. This proceduralization of exceptional state power threatens not merely the right to privacy but also more generally the rights-based framework for governance.

[208] Id. § 7–17, 36.
[209] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[210] Id. §33(2)
[211] Id. § 28–29, 33(2)

The existing legal framework is marred by a disconcerting disparity between authority and responsibility. Its emphasis on ambiguous national security rationales, lack of pre-authorization by the judiciary, and failure to provide transparency mechanisms has created an environment of unreviewable discretion. There is no effective notice, remedy, or guarantee that monitoring is finely targeted or reasonable. In this void, constitutional protections are made conditional on executive interpretation instead of legal safeguarding.

Given this, it is imperative to think through a more ethical and responsible surveillance system that incorporates constitutional morality and national security. To bridge the gap, the subsequent chapter presents concrete recommendations and reforms that can assist the Indian surveillance system in its quest to regain its constitutional legitimacy, transparency, and people's trust.

CHAPTER 6

FINDINGS AND SUGGESTIONS

This dissertation has traced the conceptual development and legal articulation of the right to privacy in India, situating it within the broader debate on the expanding scope of state surveillance. The recognition of privacy as a fundamental right under Article 21 of the Constitution marked a pivotal shift in Indian constitutional jurisprudence, reflecting a growing awareness of the need to safeguard individual autonomy and dignity in an increasingly digitised world. In the wake of landmark judicial pronouncements, India has witnessed the emergence of a privacy rights framework that aspires to balance civil liberties with state interests in security and governance.

However, the concurrent proliferation of surveillance infrastructures including centralized monitoring systems, digital identity regimes, and algorithmic profiling has foregrounded persistent tensions between constitutional ideals and executive practice. While recent legislative enactments such as the Information Technology Act, the Digital Personal Data Protection Act, and the Telecommunication Act seek to regulate the collection and processing of data, they often grant expansive discretion to state authorities, raising critical questions about procedural safeguards, legal clarity, and institutional accountability.

From a comparative and normative perspective, the dissertation has explored how India’s surveillance ecosystem aligns with international human rights obligations. Instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention on Human Rights offer rigorous tests of legality, necessity, and proportionality, yet India's domestic laws and practices often fall short of these global benchmarks. The absence of a unified, rights-based statutory framework continues to pose challenges to transparency, oversight, and democratic control over surveillance activities.

In sum, while the constitutional recognition of the right to privacy represents a normative milestone, its realisation remains contested in practice. The growing reach

of surveillance in India demands a more robust reconciliation between individual freedoms and state imperatives. As new technologies reshape the architecture of governance, the urgency of embedding privacy protections within a clear, accountable, and rights respecting legal framework becomes all the more apparent.

6.1 Findings

In modern constitutional democracies, safeguarding the right to privacy while permitting state surveillance remains a delicate balancing act. In India, this balance is tested as the right to privacy, though now recognised as a fundamental right, is not an absolute right. The Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017)[212] categorically affirmed that privacy is intrinsic to the right to life and personal liberty under Article 21. However, the judgment also laid down that the right can be reasonably restricted if the measure satisfies the tests of legality, necessity, and proportionality. Thus, privacy can be curtailed for legitimate state objectives like national security, public order, or crime prevention, provided that such restrictions are backed by law and meet constitutional scrutiny. Therefore, while privacy is fundamental, it is not inviolable or beyond limitation.

Despite this constitutional recognition, India's existing legal framework primarily the Information Technology Act, 2000, along with newer laws like the Digital Personal Data Protection Act, 2023, and the Telecommunication Act, 2023 is insufficient to safeguard individual privacy in the context of modern surveillance. These laws confer sweeping powers on the executive without corresponding safeguards such as independent judicial oversight or stringent procedural standards. Mass surveillance systems such as the Central Monitoring System (CMS), NATGRID, and state-led identity platforms like Aadhaar and DigiYatra operate with limited transparency and are not subjected to rigorous accountability mechanisms. Although the Puttaswamy judgment emphasized necessity and proportionality, statutory reforms have not adequately incorporated these principles, leading to a gap between constitutional ideals and legislative practice.

[212] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1

Moreover, India’s surveillance framework remains largely misaligned with established international human rights standards, particularly those articulated in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR) both of which India has endorsed. These instruments impose a binding obligation on states to ensure that any intrusion into an individual’s privacy is lawful, necessary for a legitimate aim, and proportionate in scope and effect. In practice, however, India's surveillance systems frequently operate without clear legislative mandates, independent oversight bodies, or transparent procedural safeguards. Unlike jurisdictions under the European Convention on Human Rights (ECHR) which require rigorous judicial scrutiny, independent authorisation, and detailed accountability mechanisms India lacks a comprehensive statutory regime to uphold these protections. This disconnect between international obligations and domestic practices undermines the principles of legality, necessity, and proportionality, exposing India’s surveillance architecture to both constitutional infirmities and international censure for failing to uphold privacy as a core democratic right.

Accordingly, the hypothesis of this study is affirmed positively - India's current laws and regulations on state surveillance inadequately balance the state surveillance needs with individual privacy rights, which could lead to violations of constitutional privacy

6.2 Suggestions

1. Institutionalize Judicial Oversight over Surveillance

One of the most significant lacunae in India’s current surveillance regime is the absence of independent judicial oversight. Under the Information Technology Act, 2000 and the Telecommunications Act, 2023, surveillance approvals rest solely with the executive, creating a situation where the same authority acts as both the enforcer and reviewer of surveillance measures. To remedy this, a statutory requirement for prior judicial authorization must be introduced for all interception, decryption, and data monitoring activities. Surveillance requests should be presented before a designated judicial magistrate or an independent privacy ombudsman, thereby ensuring an impartial assessment of necessity and proportionality. Such a system would provide much-needed checks and balances and align with constitutional principles.

2. Enact a Comprehensive Surveillance Regulation Act

India’s surveillance landscape is governed by IT Act, Aadhaar Act, and DPDP Act. These disjointed frameworks fail to provide a coherent, rights-based regime. A Comprehensive Privacy and Surveillance Regulation Act is urgently needed to consolidate all laws dealing with state surveillance, interception, decryption, facial recognition, biometric collection, and data profiling. The proposed legislation must incorporate clear definitions, explicit procedural safeguards, data retention limits, independent oversight mechanisms, and avenues for redress. This would help bridge regulatory gaps and usher in legal clarity in a rapidly digitizing surveillance infrastructure.

3. Limit Executive Discretion through Defined Statutory Criteria

Excessive discretion granted to the executive enables unmonitored exemptions and authorizations under vague pretexts like "public order" or "national security." These open-ended grounds dilute the legality and proportionality requirements essential for constitutional compliance. To address this, all executive powers related to surveillance and data access must be circumscribed by statute with narrowly defined conditions. Moreover, every exemption or order should be time-bound, specific in scope, and subject to periodic review by a judicial or legislative body. This will ensure surveillance remains an exception, not the norm.

4. Establish an Independent Data Protection Authority (DPA)

The proposed Data Protection Board under the DPDP Act lacks autonomy and accountability, being wholly executive-controlled. To ensure neutrality and efficacy, a constitutionally independent Data Protection Authority (DPA) must be established. This authority should comprise experts in law, technology, cyber security, and human rights, with appointments made through a transparent, bipartisan process. The DPA should possess powers to audit, investigate, enforce penalties, and publish transparency reports. Only such an empowered body can effectively regulate both private and governmental data processors and safeguard individual rights in the face of growing surveillance.

5. Introduce Post-Facto Notification and Right to Redress

Under the current legal structure, individuals are never informed if they were subjected to surveillance, even after the objective of such surveillance has been fulfilled. This violates principles of natural justice and the right to seek legal recourse. A post-facto notification system must be introduced, wherein individuals are informed of surveillance actions against them once the legitimate purpose ceases to exist. Such notification may be delayed if immediate disclosure compromises state interests but must eventually be mandated. Alongside, a grievance redressal mechanism must be created to enable affected persons to challenge unlawful surveillance and seek compensation.

6. Embed Procedural Safeguards and Periodic Review Mechanisms

Present surveillance laws including IT Rules, permit prolonged monitoring without independent assessment. This opens the door to misuse and normalization of surveillance. To rectify this, laws must mandate periodic judicial review of ongoing surveillance orders. Each extension should require a fresh legal assessment of necessity, proportionality, and lack of alternative means. A centralized oversight body comprising retired judges, civil society representatives, and technical experts should be constituted to monitor such extensions and publish anonymised summaries of oversight decisions, ensuring democratic accountability.

7. Codify Data Minimization and Purpose Limitation Principles

Mass surveillance programs like CMS, NATGRID, and NETRA engage in excessive data collection, often beyond the scope of the intended objective. This violates the core principle of data minimization that only the data strictly necessary for a legitimate purpose should be collected and retained. The surveillance law must mandate clear purpose limitation, explicitly stating the use-case for each data collection effort. Data collected must be deleted immediately after the purpose is fulfilled, and retention must not exceed statutory limits unless approved by a judicial authority. Such safeguards will limit abuse and ensure alignment with global privacy norms.

8. Protect End-to-End Encryption and Digital Security

Weakening encryption affects not only targeted individuals but also millions of other users whose data may become vulnerable. The law must explicitly protect the right to end-to-end encryption, permitting decryption only under judicial supervision and only in the most exceptional cases involving grave threats to national security. This would preserve the integrity of digital ecosystems while balancing state interests.

9. Reform the Aadhaar Oversight and Disclosure Mechanism

Aadhaar Act permits disclosure of sensitive biometric data in the name of national security without judicial review, overseen only by a secretarial committee. This framework lacks transparency and invites abuse. The Aadhaar Act should be amended to require prior judicial authorization for any disclosure of biometric or identity data. Additionally, oversight should be assigned to a Parliamentary Standing Committee on Surveillance or a retired judicial panel, thereby promoting accountability and public trust.

10. Mandate Parliamentary Scrutiny and Transparency Reporting

India's surveillance systems operate with no mandatory parliamentary oversight or public disclosure. This undermines democratic accountability. A Parliamentary Committee on Digital Rights and Surveillance should be constituted to review surveillance schemes, examine reports from data protection bodies, and scrutinize executive action. Additionally, all surveillance-authorised bodies must be legally obligated to publish annual transparency reports, indicating the number of requests made, approvals granted, and categories of surveillance undertaken without compromising national security.

11. Implement Puttaswamy's Proportionality Doctrine across All Frameworks

Most existing surveillance laws do not mandate a proportionality assessment prior to data interception or monitoring. As laid down in *Puttaswamy (2017)*[213], any state action

[213] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1

restricting privacy must pass the three-pronged test: legality, necessity, and proportionality. Surveillance laws should be amended to incorporate a statutory proportionality test, ensuring that every surveillance act is not only lawful but also the least restrictive means available, and that safeguards are in place to prevent abuse. No surveillance request should proceed without fulfilling all elements of this constitutional doctrine.

12. Align Indian Laws with International Privacy and Surveillance Standards

India's legal framework for surveillance falls short of international norms on the Right to Privacy in the Digital Age. To bridge this gap, Indian laws must be aligned with global standards on data protection, including obligations of notice, consent, independent oversight, and cross-border data protections. Furthermore, India should play an active role in shaping international treaties on digital privacy and commit to mutual accountability in surveillance cooperation agreements, particularly when using foreign technologies like Pegasus.

While the transition to a digital future is inevitable and offers undeniable advantages, the suitability and effectiveness of existing information privacy laws in addressing digital memory, data permanence, and breaches of informational privacy remain uncertain. These laws are often difficult to enact, face challenges in enforcement, and provide limited assurance against evolving technological risks. As states increasingly embrace digital governance, this transformation must not come at the cost of undermining the fundamental right to privacy. It is imperative that the pursuit of digital innovation be tempered with robust legal safeguards that ensure the preservation of constitutional freedoms and individual autonomy.

BIBLIOGRAPHY

BOOKS

1. Adrienn Lukács, What Is Privacy? (Ph.D. thesis, Univ. of Miskolc, 2016).
2. Akin Unver, Politics of Digital Surveillance, National Security and Privacy (Ctr. for Econ. & Foreign Pol'y Stud. 2018).
3. Anna Jonsson Cornell, Right to Privacy, in Max Planck Encyclopedia of Comparative Constitutional Law (Oxford Univ. Press 2020).
4. Clayton Northouse ed., Protecting What Matters (Brookings Inst. Press 2006).
5. David Lyon, Surveillance Studies: An Overview (Polity Press 2007).
6. Jan Holvast, History of Privacy, in IFIP Advances in Information and Communication Technology 13 (2009).
7. John Locke, Two Treatises of Government (Peter Laslett ed., Cambridge Univ. Press 1988).
8. Kathryn Henne, Surveillance in the Name of Governance (Russ. Socio. Rev. 2019).
9. Maja Galic, Surveillance and Privacy in Smart Cities and Living Labs (2019).
10. Paul Voigt & Axel Von Dem Bussche, The EU GDPR: A Practical Guide (Springer 2017).
11. Sjoerd Keulen & Ronald Kroeze, Privacy from a Historical Perspective, in The Handbook of Privacy Studies (Amsterdam Univ. Press 2018).
12. Torin Monahan, Surveillance as Governance, in Surveillance and Democracy (2010)

JOURNAL ARTICLES:

1. A. Alibeigi et al., Right to Privacy: A Complicated Concept to Review, 5 J. Pol. & L. 1 (2019).
2. Addison Litton, The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression, 14 Wash. U. Glob. Stud. L. Rev. 2015.

3. Agustín Rossi, How the Snowden Revelations Saved the EU General Data Protection Regulation, 53 Int'l Spectator 116 (2018).
4. Apar Gupta, India's Surveillance Framework and the Need for Reform, 14 NUJS L. Rev. 1, 8–12 (2021).
5. Apar Gupta, The Supreme Court's Right to Privacy Decision: Reading Between the Lines, 12 Indian J. Const. L. 55, 67–69 (2018).
6. Arghish Akolkar, Government Surveillance Against the Right to Privacy in Matters of Cyberspace in India, 5 Elec. J. Soc. & Strategic Stud. 38 (2024).
7. Ashley Deeks, An International Legal Framework for Surveillance, 55 Va. J. Int'l L. 291 (2015).
8. Chinmayi Arun, AI and the Right to Privacy in India: Emerging Constitutional Questions, 3 Indian J. Const. L. 111, 115 (2020).
9. Dorothy J. Glancy, The Invention of the Right to Privacy, 21 Ariz. L. Rev. 1 (1979).
10. Gautam Bhatia, State Surveillance and the Right to Privacy in India: A Constitutional Perspective, 26(1) Nat'l L. Sch. India Rev. 127, 139–40 (2014).
11. Harsh Bansala, Road to Become a Surveillance State, U.S. Corpus L.J., Sept.–Nov. 2021.
12. Keigo Komamura, Privacy's Past: The Ancient Concept and Its Implications for the Current Law of Privacy, 96 Wash. U. L. Rev. 1337 (2019).
13. Kush Kalra, Right to Privacy Under Indian Constitution, 2 GIBS L.J. 38 (2020).
14. Mohd Faiz Khan & Naseem Ahmed, The Erosion of Privacy in the Face of State Surveillance: A Digital Dystopia, 29(1) Madhya Pradesh J. Soc. Sci. 438 (2024).
15. Murni Wan Mohd Nor & Ratnawati Mohd Asraf, Technology and the Deterioration of Right to Privacy, 7 Int'l J. Asia Pac. Stud. 37 (July 2011).
16. Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934 (2013).
17. Paul Rosenzweig, The USA Patriot Act and Privacy: A New Frontier of Surveillance, 13 Stan. Tech. L. Rev.1 (2010).
18. Payal Thaorey, Legal Introspection Towards the Development of Right to Privacy as Fundamental Right in India, 11 Indonesia L. Rev. 3, art. 5 (2021).
19. Ramkant Tripathi, Evolution of Right to Privacy in India: National and International Perspective, 7 J. Crit. Rev. 300 (2020).
20. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

21. Sandeep Bhushan, Paper-Thin Safeguards and Mass Surveillance in India, 50(22) Econ. & Pol. Wkly. 10 (2015).
22. Sargam Thapa, The Evolution of Right to Privacy in India, 10 Int'l J. Human. & Soc. Sci. Invention, Feb. 2021.
23. Sheetal Asrani-Dann, The Right to Privacy in the Era of Smart Governance, 47 J. Indian L. Inst. 53 (2005).
24. Soujaatyaa Roy, The Impact of the Recent Pegasus Spyware Controversy on the Right to Privacy in India, 6 Int'l J.L. Mgmt. & Human. 1060 (2023).
25. Tejas Jindal, Right to Privacy as a Fundamental Right in India: Evolution, Challenges and the Impact of Digitalization, Int'l J. for Multidisciplinary Res., Nov.–Dec. 2024.
26. Usha Ramanathan, State Surveillance and the Right to Privacy in India, 50(22) Econ. & Pol. Wkly. 12 (2015).
27. Usha Ramanathan, Unique Identification: Inclusion and Surveillance in the Indian Biometric Scheme, 52(7) Econ. & Pol. Wkly. 61 (2017).

STATUTES AND INTERNATIONAL INSTRUMENTS:

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, Acts of Parliament, 2016 (India).
2. Constitution of India, art. 21.
3. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.
4. Convention on the Rights of Persons with Disabilities, Dec. 13, 2006, 2515 U.N.T.S. 3.
5. Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.
6. Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
7. G.A. Res. 217A (III), Universal Declaration of Human Rights (Dec. 10, 1948).
8. Indian Post Office Act, No. 42 of 2023, Acts of Parliament, 2023 (India).
9. Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
10. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Dec. 18, 1990, 2220 U.N.T.S. 3.

11. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
12. International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3.
13. Telecommunication Act, No. 44 of 2023, Acts of Parliament, 2023 (India).
14. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (U.S.)

ONLINE SOURCES:

1. Constituent Assembly Debates, Vol. 3 (Apr. 30, 1947), https://www.constitutionofindia.net/constitution_assembly_debates/volume/3/1947-04-30.
2. Constituent Assembly Debates, Vol. 7 (Dec. 3, 1948), https://www.constitutionofindia.net/constitution_assembly_debates/volume/7/1948-12-03#7.66.11.
3. David Harrington, U.S. Privacy Laws: The Complete Guide, VARONIS, https://www.varonis.com/blog/us-privacy-laws#us-data-privacy-law-timeline.
4. Disha Verma, *Digi Yatra:* A Service or Surveillance?, The India Forum (Feb. 8, 2024), https://www.theindiaforum.in/article/digi-yatra-service-or-surveillance.
5. Kamesh Shekar & Shefali Mehta, The State of Surveillance in India, ORF (July 4, 2023), https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india.
6. Tathagata Satpathy et al., Are India's Laws on Surveillance a Threat to Privacy?, The Hindu (Dec. 27, 2018), https://www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25844250.ece.
7. Ujwala Uppaluri, The Privacy Hearings: Notes on Supreme Court Practice, Law and Other Things (July 22, 2017), https://lawandotherthings.com/2017/07/the-privacy-hearings-some-notes-on-supreme-court-practice.

REPORTS:

1. Data Security Council of India, Legal Framework for Data Protection and Security and Privacy Norms (Apr. 10, 2025), https://www.dsci.in/files/content/knowledgecentre/2023/Legal%20Framework%20for%20Data%20Protection%20and%20Security%20and%20Privacy%20norms.pdf.
2. Jhalak M. Kakkar et al., The Surveillance Law Landscape in India and the Impact of Puttaswamy (Nat'l L. Univ. Delhi 2023).
3. Maria Xynou & Elonnai Hickok, Security, Surveillance and Data Sharing Schemes and Bodies in India.
4. Mira Swaminathan & Arindrajit Basu, *S*urveillance and Data Protection: Threats to Privacy and Digital Security (2020).
5. Sangeeta Mahapatra, Digital Surveillance and the Threat to Civil Liberties in India, GIGA Focus Asia, No. 3 (May 2021).
6. U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014).