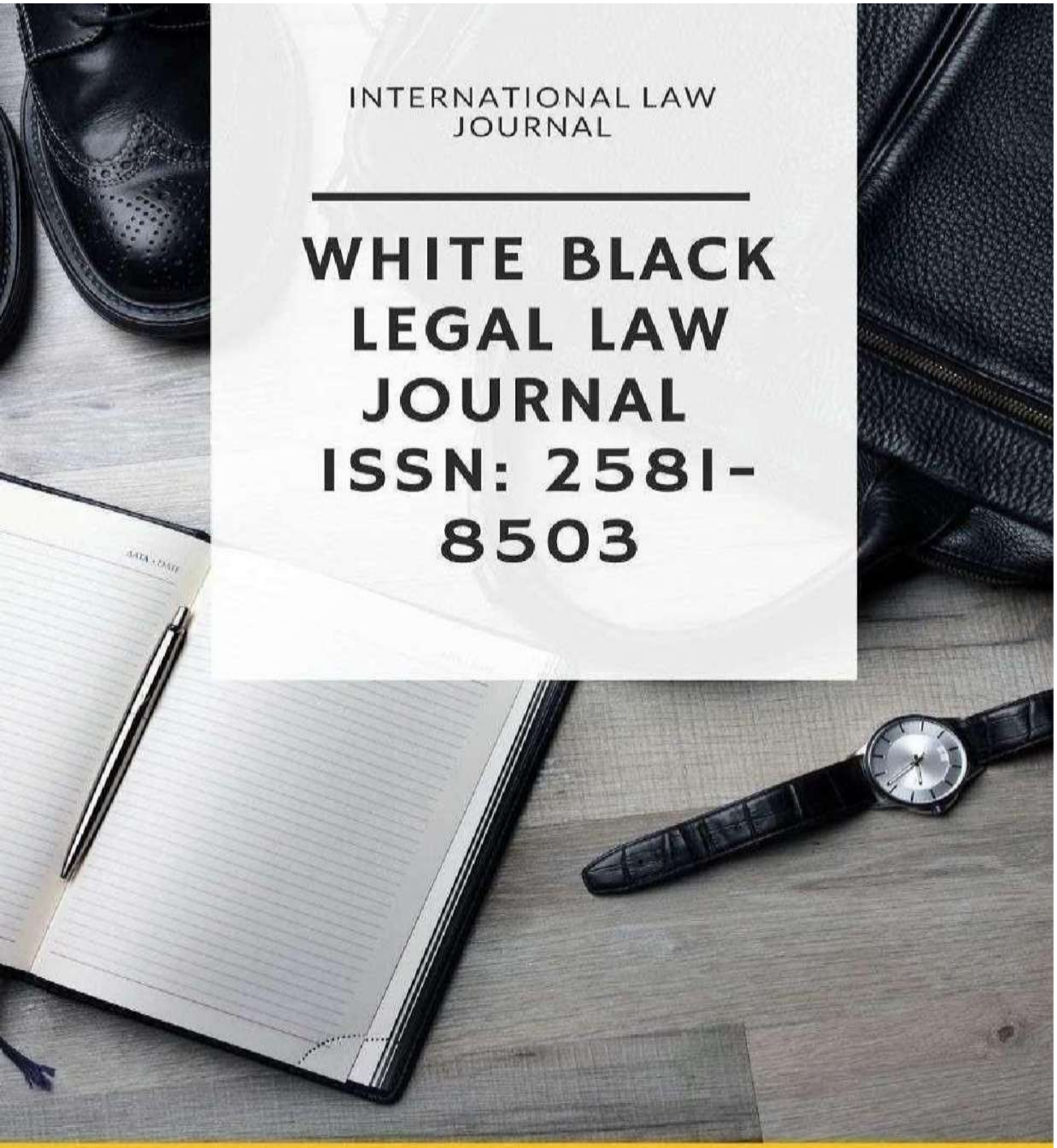

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DATA PRIVACY IN THE DIGITAL AGE: BALANCING SECURITY AND INDIVIDUAL RIGHTS

AUTHORED BY - HEMASHREE B & DR. SEENA NAIR

CHAPTER 1

1. Introduction

The protection of privacy involves protecting the individual's private data[1] from being gathered, used, processed, disclosed, or exploited by third parties, including individuals, private entities, or governmental agencies. The rise in digital communication and digital data processing, for monetary transactions and service delivery, has made the personal data the most precious asset of modern societies, and there has been an exponential increase in its generation, storage, and processing as individuals rely on digital platforms to communicate, transact business, and access services offered by the government and private sectors. In other words, the massive volume of personal data creation, storage, and processing has triggered the requirement for a legal framework to guarantee the individual's right to privacy of data from exploitation by third parties

Personal data can include (though not limited to) name, address, birth date, governmental identification number, medical number, banking details, health record (disease), geographical area (place of living), electronic mail (history) and prior search type (types) performed. The access to this information without the person's authorization could lead to various harmful outcomes, including identity theft, cybercrime, tracking, profiling or different kinds of discrimination. Thus, one of the key aspects of data privacy is the provision of individuals with the opportunity to regulate the manner of collecting and disseminating their personal information by governments/private companies. One of the key aspects of data privacy is informational self-determination. It means that an individual determines whether he/she wants his/her personal information to be disclosed to third parties or not.

2. Evolution of Privacy Rights Globally and in India

From being considered a social norm concerning personal space, privacy has been transformed into a legal right[2] that has been accepted globally as a basic human right within modern

[1] Alan F Westin, *Privacy and Freedom* (Atheneum 1967).

[2] Universal Declaration of Human Rights 1948, art 12.

democratic societies. At first, privacy was defined mainly in terms of freedom from the physical invasion of the individual by another person, where such invasions occur within the individual's private residence or during their activities. The advancement in technology and the growing capabilities of the State to conduct surveillance, however, resulted in privacy being extended to cover the right to protect personal information and make decisions freely. In addition, privacy can be viewed in relation to the preservation of human dignity and liberty, thus necessitating its protection through national and constitutional law.

The fundamental human right to privacy is stated under Article 12 of the Universal Declaration of Human Rights, which was proclaimed in January 1948, and Article 17 of the International Covenant on Civil and Political Rights, which came into effect in December 1966. Both these articles lay down provisions for safeguarding individuals from all arbitrary interference into their private life. These international conventions have served as the foundation for the establishment of global laws on privacy. In India, the legal right to privacy has been accepted by the judiciary because there is no provision for it in the Constitution. The legal right to privacy in India has gained judicial acceptance from 1963 when the judgment of Kharak Singh v. State of Uttar Pradesh[3] was delivered, then continuing in other judgments like Gobind v. State of Madhya Pradesh (1975)[4], R. Rajagopal v. State of Tamil Nadu (1994)[5], and PUCL v. Union of India (1997)[6].

3. Importance of Data Protection in the Digital Era

The protection of data has been growing to become a very relevant topic in our contemporary society due to the fast-paced emergence of internet connections and various technological innovations in e-Government and other services. People share their personal information with numerous services such as e-Banking, health facilities, educational institutions, social networks, and government institutions. The introduction of these innovative technologies has made the service provision more accessible and efficient for people, although it comes with a set of risks of misappropriation of data by a third party, including threats to security of an account, identity theft, and cybercrime such as fraud and vigilantism.

From the famous case of Justice K.S. Puttaswamy v Union of India (2017)[7], it was established by the Supreme Court of India that the concept of right to privacy includes the right of a person

[3] *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.
[4] *Gobind v State of Madhya Pradesh* (1975) 2 SCC 148.
[5] *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632.
[6] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.
[7] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC).

to the protection of their personal data, and proper legislative measures to protect personal data will result in greater autonomy for individuals, build up consumer trust in the use of digital services, and contribute to economic development. This shows that there must be strong protective measures put in place.

4. Need for Data Protection Laws in India

As far as digitization in India is concerned, there have been a number of developments regarding the digitization of citizen data. These include digitization projects such as Digital India, Aadhar, online banking, and internet services to all, making it easier for services to be delivered to the citizens more efficiently. Owing to this fast-paced process of digitization, a large volume of personal data has been gathered and processed both directly and indirectly by the government and its agencies.

Prior to 2017, India did not have any strong data protection laws in place. With the implementation of the Information Technology Act in 2000[8], some data privacy was offered to the individual while further restrictions were imposed via the 2011 Internet rules. Thus, an individual did not really have much recourse at his disposal if his or her data was ever mishandled.

In the case of Justice K.S. Puttaswamy v Union of India, it was determined that the right to privacy was a fundamental right and that more needs to be done to ensure that individuals have their rights protected in terms of data protection.

The introduction of the Digital Personal Data Protection Act (DPDPA), 2023[9] can be seen as taking a substantial step towards ensuring that the standards/measures necessary to ensure the protection of individuals' rights are increased. Nonetheless, issues pertaining to the implementation of the DPDPA and exemptions from following the provisions of the DPDPA granted to Government Agencies indicate that protecting individuals' basic/legally protected rights is still a problem.

[8] Information Technology Act 2000.

[9] Digital Personal Data Protection Act 2023.

5. Research Problem

With the rapid development of digital technology, the manner in which personal data is acquired, processed, and stored by both the government and private corporations has drastically been transformed. Most individuals make use of digital technologies for communicating, banking transactions, health care, education, and social services among others. While the developments in technology have revolutionized the delivery of services in many sectors, these same advancements have posed many challenges when it comes to ensuring that individuals' data is secured against any misuse. Data acquisition without proper regulation puts data subjects at risk of;

Another issue of concern is the fact that in India, no such legal framework exists for the protection of personal data over several decades due to the development of the technologies and expansion of the digital delivery systems, though this framework was desperately required. The only existing legal framework is the Information Technology Act of 2000, which contained several provisions concerning the protection of personal data. However, these provisions could not create an adequate legal framework regulating the collection, use, and processing of personal data in the digital environment. In 2017, the Supreme Court of India recognized the right to privacy as a fundamental right of people protected by Article 21 of the Indian Constitution.

6. Research Questions

Whether the recognition of the right to privacy as a fundamental right under Article 21 of the Constitution provides adequate protection for personal data in the digital environment?

Whether the Digital Personal Data Protection Act, 2023 effectively regulates the collection, storage, and processing of personal data by public authorities and private organizations?

Whether the rights granted to data principals under the Digital Personal Data Protection Act, 2023 ensure meaningful control over personal information and accountability of data fiduciaries?

whether surveillance mechanisms under the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 operate within constitutional limits and provide adequate safeguards for informational privacy?

Whether international frameworks such as the European Union's General Data Protection Regulation (GDPR) provide useful guidance for strengthening India's legal framework in balancing national security and individual privacy rights?

7. Hypothesis

The present research is premised on the assumption that the recognition of privacy as a fundamental right under Article 21 of the Indian Constitution has greatly enhanced the laws and regulations in respect to the protection of personal data in India. At the same time, it maintains that both the government and private entities' accountability in the processing of personal data through institutional mechanisms that are robust enough to provide for effective implementation of privacy safeguards is critical to achieving successful implementation of privacy safeguards.

Furthermore, the study assumes that the Digital Personal Data Protection Act, 2023 marks a significant legislative advancement with respect to providing for rights of individuals and obligations of data fiduciaries. It is also accepted that certain parts of the DPDPA 2023 require additional strengthening in order to provide for effective protection of informational privacy, especially regarding government exceptions and the independence of authority.

It is also assumed that national security-related measures utilized for surveillance must be constitutional and that they must also meet the requirements of legality, necessity, and proportionality. Therefore, it will be necessary to provide for an appropriate balance between the interests of national security and the right of individual privacy through transparent regulatory frameworks, individual oversight by the judiciary, and institutional accountability.

8. Objectives of the Study

This research will evaluate both national and local constitutional recognition of data privacy rights under Indian law in an age where technology is ever-changing and there is an increased reliance on digital forms of communication. As the number of electronic service delivery mechanisms in many sectors continues to grow due to increased digital governance, a significant legal and constitutional issue is how to protect individuals' personal data. Thus, the purpose of this research will be to define and assess the meaning and significance of privacy as a fundamental right that must be afforded protection under Article 21 of the Constitution; and therefore to provide an understanding of how privacy provides individuals protection from losing control over their own information in an age characterised by digital technologies.

A second focus of this study will be to evaluate the applicable statutory framework in India regarding the collection, storage, and processing of data, focusing specifically on the provisions of the Information Technology Act 2000 and the Digital Personal Data Protection Act, 2023. This evaluation will provide an understanding as to whether these two Acts' legal protections cover consumers who are subjected to unreasonable protections for their data by third parties that collect, store and process their data without consent or knowledge.

Furthermore, the study will analyse how effectively fiduciaries have a legal responsibility (fiduciary duty) to their data

9. Research Methodology

The current study uses a doctrinal research method for legal studies using mainly the analysis of statutory provisions, constitutional provisions, judicial opinions and scholarly writing related to the protection of information and personal data privacy. The doctrinal research method is considered particularly appropriate for examining fundamental rights and legal principles governing these rights because it will provide for the systematic interpretation of statutory provisions and constitutional provisions in context to the applicable judicial decision and development of the law. The current study used the doctrinal research method to analyse

the evolution of jurisprudence on privacy in India as well as for analysing the effect of statutory measures governing the protection of personal information in the digital context.

The present research relied heavily on primary legal sources including the Constitution of India's provisions, especially Article 21 of the Constitution of India providing for protection of life and personal liberties, and statutory provisions including the Information Technology Act of 2000 and the Digital Personal Data Protection Act, 2023. Additionally, the judgements of the Supreme Court and other High Courts on the recognition and the protection of Privacy Rights have been reviewed and examined to provide insights into the Constitutionally recognised basis for the right to privacy in India. Judgements of significance with respect to privacy jurisprudence include Kharak Singh v. State of Uttar Pradesh; Gobind v. State of Madhya Pradesh; People's Union for Civil Liberties v. Union of India; the judgement of M.P. High Court in Computer Society of India v. State of Madhya Pradesh; and Puttaswamy (Retd.) v. Union of India.

10. Scope and Limitations of the Study

The goal of this study is to concentrate on the constitutional and statutory rules governing the protection of personal data in India while the digital era comes to fruition and electronic governing systems are created at the same time. The research will focus primarily on analyzing how privacy law has developed under Article 21 of the Constitution, as well as how legislative measures like the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 help provide a legal framework for protecting privacy in India. These two acts make up the bulk of the regulations that govern how personal information is processed in India. Thus, they are the primary focus of this study.

The study will also look at the legal basis for surveillance under the current laws provided by the Indian Telegraph Act of 1885 and the Information Technology Act of 2000 to evaluate their effect on information privacy. Because surveillance powers are often justified based upon the needs of national security or the maintenance of public order, the research will also try to determine if they operate within the limits of the Constitution and if there are sufficient measures in place to prevent arbitrary violation of individual liberty through these powers. Finally, the research will consider the relationship between national security and any rights under the Constitution to be guaranteed in the electronic environment.

To provide additional substance to the analysis conducted in this study there will be limited references made to comparative analysis.

11. Scheme of the Study

The research study has been separated into six main chapters so that the structure and content can be presented clearly and completely in one location for the reader. Each chapter looks directly at the relationship between data privacy and national security within the rapidly changing technological environment and the growing use of digital governance systems.

In Chapter One, an explanation of data privacy is provided. This chapter will discuss the evolution of privacy rights on a global and Indian level. This chapter consists of a definition of the problem of study; a list of key research questions; a reasonable hypothesis for each primary objective; and a brief history of the methodology used to conduct the survey as well as its scope and any limitations.

In Chapter Two, the constitutional framework by which data privacy is protected will be provided; particularly, the rights outlined in Article 21 of India's Constitution. Chapters Two to Five will look at how important judicial decisions have developed privacy jurisprudence and how the recognition of privacy as a fundamental right has enhanced the protection of individual's ability to maintain their dignity when using digital media in the 21st century.

In Chapter Three, the appropriate statutory laws relating to the protection of personal data in India will be examined (primarily the Information Technology Act of 2000, as well as the Digital Personal Data Protection bill which is expected to be passed in the 1st Quarter of 2023).

CHAPTER 2

CONSTITUTIONAL FRAMEWORK OF RIGHT TO PRIVACY IN INDIA

1. Concept of Privacy under the Constitution

Privacy in India was never considered as an explicit fundamental right in the Constitution. Rather, the judiciary determined the concept of privacy in its rulings in various cases over time. Though privacy cannot be found in the constitutional text as a fundamental right, it was found embedded in some other fundamental rights by the judiciary. The apex court declared that privacy is an aspect of life that goes with being able to live fully. Laws evolve as society does and is influenced by advances in technology.

Dignity, for its part, is bound up with maintaining personal space – liberty is maximized when the decisions made remain personal within institutions founded on joint governance. From a judicial perspective, privacy has been understood as protecting the details of life, the close relationships, the communications, and personal information from unexpected interference on the part of power. Privacy divides into several aspects: bodily privacy, spatial privacy, and informational privacy. Unwanted physical contact and compulsory medical procedures are violations of privacy that have been recognized as such universally within legal theory. In this realm, the right to be free of prying in the place where walls are supposed to serve their purpose is provided by spatial privacy. The advent of surveillance technology brought in informational privacy – the right to regulate who knows what about oneself.

Within the view of legal theory, privacy is an immutable bulwark against the encroachment of power when it comes too close. The courts often refer to secluded areas in which one's identity forms and flourishes when mentioning the right to liberty. There are certain eyes that do not deserve to witness our development. Dignity is never about grandiose gestures; rather, it lies in the ability to conceal things. One's autonomy is reflected in one's control over their life.

With the rise of technological development in this day and age, the problem of the protection of private information grows increasingly important, especially as the government is implementing more services online and becomes dependent upon them. The construction of such systems as national databases, internet-based archives or portals entails a significant collection of personal information.

Though these technologies may contribute to accelerating bureaucratic processes, they do offer a chance of abuse, alongside their potential for monitoring people. Therefore, it becomes imperative to treat privacy as a fundamental right in controlling technological progress. Out-of-court decisions in the development of privacy law indicate the adaptability of the constitution in the wake of new technology in transforming people's lives. The courts view privacy as an essential aspect of liberty, hence giving it greater protection. Personal information is now better safeguarded against abrupt seizures by authorities.

2. Article 21 and Personal Liberty

Article 21[10] of India's Constitution states that life and liberty cannot be deprived of a person unless there is a procedure established by law. Although the provision may appear brief, through judicial interpretations over the years, it is now seen as an effective protection of fundamental rights. However, back in 1950, the Supreme Court interpreted Article 21 of India's Constitution in a manner whereby freedom could be restricted if such was regulated by a rule, no matter how oppressive it might be.

Nonetheless, everything changed after the Supreme Court revised its interpretation of Article 21 of India's Constitution in the case of Maneka Gandhi v Union of India[11]. This judgment held that the procedures involved must be just and reasonable since they should be equitable, measured and humane. The interpretation led to the evolution of freedom under the Constitution. As a result, the scope of fundamental liberties was broadened to encompass needs for living in dignity. Following that case, other rights have evolved from Article 21 of the Constitution. They include rights to livelihood, health, education, environment, privacy, among others.

The characterization of privacy as an aspect of individual liberty strengthened constitutional protection in the case of government intrusions into individual lives in the absence of reasonable justification. In that context, because the courts considered the broader scope of individual liberty, elements such as private communications, data management, and self-determination received constitutional protection. Any curtailment of privacy had to ensure fairness at all times, without exception, to qualify under constitutional standards.

[10] Constitution of India 1950, art 21.

[11] *Maneka Gandhi v Union of India* AIR 1978 SC 597.

The importance of privacy cannot be understated, especially with regard to online activity, where the significance of Article 21 increases owing to the collection of large volumes of personal data by governments and organizations. The use of technology to address fundamental necessities, including the payment of bills, visiting doctors, or participating in distance learning, requires the exercise of privacy as a component of individual liberty

However, in Justice K.S. Puttaswamy vs. Union of India in 2017, the apex court upheld the protection under Article 21 for private information. As such, the concept of privacy was recognized as an essential component of liberty by the verdict. The idea of dignity persists in the preservation of one's freedom to make his own decisions. In contemporary democracies, there is a need for boundaries even more so than before due to the ubiquitous presence of technology. In anticipation, courts acted, bringing digital privacy within reach of constitutional protection. Information moves much faster today, necessitating additional weight be given to old boundaries. The practice of surveillance of citizens via networked communication led to legal deliberation, leading to the modification of already existing civil rights. As such, legal protections intended for tangible spaces were made applicable to virtual communications, too. Laws should adapt to the evolution of technology in real time while maintaining the integrity of their core purpose. Thus, an important perspective change came about.

3. Evolution of Privacy through Judicial Interpretation

It took many years since India became independent before the Indian courts started considering privacy as a constitutional right in its jurisprudence. This process happened gradually as the court interpreted laws in relation to privacy without declaring them outrightly. Since there is no article that mentions privacy under fundamental rights, the courts had to interpret privacy within the scope of existing articles like Article 21. New developments like technological advancements were incorporated in this interpretation process.

Initially, the Kharak Singh v. State of Uttar Pradesh (1963)[12] case raised issues about the infringement of personal space in surveillance by the state in practices such as night domiciliary searches. Although most judges refrained from labeling privacy as a fundamental right, they declared certain practices unconstitutional as violations of freedom of movement. However,

[12] *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.

this judgment implicitly paved the way forward, acknowledging that the invisible invasions of one's privacy may undermine Article 21-protected rights.

Advances were made in the landmark judgment of the Supreme Court in Gobind v. State of Madhya Pradesh (1975)[13]. Here, the court considered privacy to be an integral part of personal liberty but not immune to justifiable restrictions for greater social benefit. This was the first time that such a guarantee of privacy was recognized as being fundamental in nature. The necessity of protection is warranted where there is justified interference by the state.

Rulings in the courts later expanded on the concepts already established in the country. In R. Rajagopal v. State of Tamil Nadu (1994)[14], it was ruled that citizens could prevent information concerning their lives from being released if they had not given prior consent for this purpose. Similarly, People's Union for Civil Liberties v. Union of India (1997)[15] recognized that telephone surveillance is an invasion of privacy. Rather than letting things be done without limits, guidelines were created for interception in accordance with the Indian Telegraph Act.

Slowly but surely, the decisions of the higher benches started forming a better framework for the protection of personal information, which shows how much importance was gradually given to this issue in court decisions. It was only after a key ruling in Justice K.S. Puttaswamy v. Union of India (2017) that the top bench clearly declared privacy to be an essential aspect of life and liberty under Article 21. This landmark ruling was not achieved suddenly but came as a result of many years of development.

4. Justice K.S. Puttaswamy v. Union of India (2017): Constitutional Significance

Another landmark in the process of developing laws in India can be seen in the case of Justice K.S. Puttaswamy v. Union of India[16] that was heard at the Supreme Court in 2017. The matter arose due to the implementation of the Aadhaar program that collected biometric data of countless Indians. A fundamental question of whether privacy rights are protected by the Constitution of India raised. To answer such a serious issue, the Supreme Court created a special bench consisting of nine justices who would only interpret and analyze the constitution.

[13] *Gobind v State of Madhya Pradesh* (1975) 2 SCC 148.

[14] *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632.

[15] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

[16] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC).

Privacy is considered an essential part of the set of rights guaranteed by Article 21 of the Constitution. Privacy cannot be separated from other basic rights provided for in Part III of the document. Among the key arguments was the relation between privacy and human dignity. Autonomy and choice require boundaries – the ones that are established by personal privacy. When these boundaries are in place, one may follow his or her path. They are invisible, yet crucial for the protection of a democratic state, where individual liberties are paramount.

Notable among the results was the recognition of the right to informational privacy as a right to privacy in general. In light of technological developments, information networks have become more extensive, prompting worries about unauthorized access to personal data. The ability to control one's own information is seen as a crucial factor according to the decision, while protective measures are the duty of states, as far as ensuring the absence of an unlimited intrusion goes. These kinds of privacy interests require special treatment in light of contemporary digital technologies.

On the other hand, the decision explicitly stated that the right to privacy has its limitations, especially when restricted by law for public interest purposes such as protection of safety, public order, or prevention of crimes. With respect to those cases, a new approach appeared in the form of a judicial doctrine of proportionality – which would determine the legitimacy of restrictions on the basis of the presence of three criteria: legality, necessity, and balance.

After recognizing privacy as a fundamental right in the Puttaswamy case, there was a foundation for bringing extensive data privacy legislation within the country of India. Rather than only pointing out the need for reform, the decision led the path towards the creation of the Digital Personal Data Protection Act of 2023. With the use of legal logic from the perspective of dignity and autonomy, steps were taken to create legislation. Since previous attempts at reforms had failed, this was essential.

5. Privacy as Part of the Fundamental Rights Framework

The recognition of privacy as part of the bundle of basic rights brought about a new legal perspective on the matter in India. Prior to the decision in Justice K.S. Puttaswamy v. Union of India (2017), it was regarded as an indirectly guaranteed right under personal liberty in Article 21. Nevertheless, the Supreme Court clarified that its foundation does not lie solely

within one article, being closely associated with several provisions, including those of Part III – Articles 14, 19, and 21[17].

In terms of equality before the law, Article 14 and its connection to privacy also involve restrictions from arbitrary governmental actions. The infringement of an individual's personal information is considered unjust when it occurs without proper justification, and discrimination takes place whenever it affects only certain individuals while leaving others untouched. The significance of privacy in relation to Article 19 rights, which include free speech, freedom of movement, and assembly, can be explained by the importance of having personal boundaries intact for such freedoms to exist.

The issue of data handling becomes crucial for discussion not only because of its direct relation to individuals' concerns but also due to its connection to rights enshrined in the constitution. The interpretation of constitutional laws is always evolving alongside technological development, thus allowing judges to adjust the scope of rights. This happens, for example, when new methods of surveillance become common, which requires changes in the court's approaches. Rather than applying the fixed understanding, judges adopt a dynamic approach through step-by-step cases. What was previously overlooked becomes critical for the protection of the individual's autonomy. Even collection of data by state agencies raises issues of proper use of that data. However, corporations also have a great impact on the issue since private companies store users' data on a large scale. It causes a reconsideration of some long-held beliefs concerning the duties of states. In this respect, privacy becomes an inseparable component of the system of protection of individual dignity.

If privacy were a basic right, the Supreme Court concluded, then restrictions on personal data would be unacceptable without satisfying standards based on principles of justice - balance, rationality, and moderation.

6. Role of Judiciary in Protecting Informational Privacy

Since the early judicial decisions, there have been developments in terms of viewing private data from a legal perspective in India. Rather than being bound by literal interpretation, judicial

[17] Constitution of India 1950, arts 14, 19, 21.

decision-makers have considered other approaches in order to preserve personal limits. In the long run, landmark judgments played a huge role in establishing an understanding of privacy. It was through piecemeal recognition that a notion of privacy emerged as entitlement for oneself. Judicial decision-making processes varied; some were gradual while others had drastic changes in approach. This development occurred even without a definitive right stated in black and white. Interpretation provided solutions when there was ambiguity. Legal developments responded to any intrusion, as new threats came to light. Key events showed growing realization at the topmost level. Each judicial decision accumulated in building the protection of individuals.

One of the first times that the court took steps to protect personal information was in the case of R. Rajagopal v. State of Tamil Nadu (1994), wherein it declared that individuals have a right to prevent the unauthorized revelation of information regarding their personal existence if no authorization is given. Shielding personal information, according to such decisions, is important for autonomy in a democratic society. Another example of the recognition of rights to privacy was People's Union for Civil Liberties v. Union of India (1997) wherein wiretapping was considered an infringement of privacy, and protocols of limiting it were determined via the Indian Telegraph Act.

The decision made in the case of Justice K.S. Puttaswamy v. Union of India in 2017 stated that privacy was a fundamental constitutional right. It was important that control is established regarding how personal data is shared. Wherever there are restrictions to private life, they have to be justified with legality, necessity, and proportionality. As a result of the above decision, individuals using their personal data in today's digital age will receive additional protections. Apart from confirming that privacy was a fundamental right, judgments have been made concerning the issue of monitoring and the need to adhere to constitutional parameters. Wherever the state utilizes surveillance mechanisms, it is important that there are procedures, and judges must oversee these actions. There is an underlying influence that arises from these judgments, which involve collective safety and privacy

CHAPTER 3

DATA PROTECTION LAWS IN INDIA

1. Information Technology Act, 2000

The Information Technology Act, 2000 became the country's first major statute[18] concerning digital transactions. It established that computer-based records would be considered as valid documents. Although it mainly focused on supporting electronic commerce, it covered a number of different issues related to the internet and digital transactions. Privacy did not become the focus of attention of this act, although some clauses of it helped establish rules for handling of personal information in the future. Some clauses of the act indirectly became involved in establishing baseline requirements for data handling by companies. The development of technologies also led to the development of interpretation of the act. Although its language was not contemporary, its influence was expected to remain in the future. Electronic transactions had legal certainty because of the act. However, there were some gaps in the act that could be detected in the course of time.

Section 43A[19] of the Information Technology Act is related to protecting personal information. This act provides for penalties to be applied to corporations that do not use adequate security while working with their data. The lack of sufficient protection leads to the damage or unmerited benefits.

However, apart from the above provision, another one is Section 72[20], whereby anyone accessing any electronic record in a lawful manner and disclosing any information in an illegal manner faces punishment. In such a case, as confidentiality has been breached, a person should face the relevant sanctions according to this provision. Handling of electronic records cannot be taken lightly by the Act, since confidentiality of people's information is only possible if people believe in their handling. Although legislation on data protection did not come into being fully, some provisions showed high legal value in safeguarding citizens from different

[18] Information Technology Act 2000.

[19] Information Technology Act 2000, s 43A.

[20] Information Technology Act 2000, s 72.

types of exploitation. Personal information protection was prioritized before developing any policy governing it.

On the other hand, through Section 69[21], the Information Technology Act grants the Government of the Central and State surveillance authority. This power enables the interception of information, surveillance, and decryption of information stored electronically based on considerations of national integrity, security of territories, security of states, maintenance of public order, and investigation of crime. These provisions help in fighting cyber crimes and achieving stability, although they raise concerns about privacy infringement in the absence of tight restrictions

Although it cannot be doubted that the Information Technology Act is a vital law, being the first one to be enacted in the nation with regard to digital communication, the extent of its intention with regard to safeguarding the data of individuals is narrow since the primary emphasis of the act is not on how individual data would be handled but on ensuring that any online transaction would be regulated and any cybercrime would be prevented.

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

According to the Information Technology Act, 2000, the provisions relating to reasonable security practices in 2011[22] were set forth in order to enhance the security procedures involving personal information maintained by firms that conduct their operations online. Without setting forth such provisions, the classification of various categories of sensitive personal information was not possible. With the use of technology in organizations, there was a need for taking up some duties when dealing with such information. Even though the provisions were more aimed at non-governmental organizations, their effects went beyond future policymaking procedures. Privacy law initiatives in India gained much input from the above legislations.

Among the main changes made by the provisions of 2011 was the classification of sensitive personal information that required enhanced security precautions. The first type of personal information protected by the provision was authentication information. Financial information

[21] Information Technology Act 2000, s 69.

[22] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

including banking and credit information formed the second category of information. The third category was related to health care matters.

According to these principles, those collecting sensitive personal information in the electronic format were supposed to perform some specific functions. They had to obtain prior consent from the person from whom the data was going to be collected. Openness should have been observed; therefore, every person was supposed to receive definite answers regarding why the information was collected and what purposes it was going to be used for. It was important to provide sufficient security; this should ensure no unpermitted exposure, modification, or abuse of the collected personal information.

However, despite all the strict security measures provided above, the application of these Rules of 2011 was somewhat limited since there were certain shortcomings in the system itself. To begin with, these regulations were applicable only to private organizations which means public organizations involved in the handling of substantial amounts of personal data were not covered. Secondly, the implementation of these principles became rather difficult due to the absence of any controlling body exercising its power.

3. Digital Personal Data Protection Act, 2023

In 2023, there was enactment of a new legislation pertaining to personal data that is in digital form. The move was triggered by the precedent-setting ruling made in the case of Justice K.S. Puttaswamy v. Union of India. As a result of this ruling, the need arose to ensure that all the information that had been provided in digital forms should be secured. Different from other laws which involved uncertainties, there was now certainty on the way that individuals' data would be controlled. In contrast to the previous approach, where the management of information was not certain, it was necessary to make the laws in the wake of increased threats.

Information that belongs to a particular person and is processed either by the government or private organizations called data fiduciaries comes under the scope of this law. There will be procedures followed when handling the information, such as avoiding unnecessary use of information, safekeeping, and allocation of fault in the event of error. Information gathered has specific uses that should be aligned with the permission granted by the information's owners. There will be agreements made in the process of setting up the system in regard to flow of

information. It is relatively easy to give individuals more control on their personal information due to the openness of the system.

It is notable about this act that it takes into consideration the claims of individuals known as data principal about the use of their personal information. Besides allowing access to the process used in utilizing the information, any errors in the process can be corrected. If information is no longer applicable for the intended use, it can be deleted. The removal of personal information is not prohibited after a user gives consent to allow usage of their information.

Also mentioned in the act is the creation of the Data Protection Board of India that will take care of enforcing compliance with the obligations stated under the law as well as handling issues regarding the use of data. In the event of violations of the act, there will be investigations conducted before penalties are imposed on violators. The creation of such board is another significant move in ensuring that India maintains digital privacy through proper regulation.

However, in its Digital Personal Data Protection Act for 2023[23], the government of India understands that there is a need to strike a balance between the protection of individual's privacy and data, especially those provided voluntarily, and the responsibilities of the government in ensuring security, order, and prevention of crimes. Hence, there are some exceptions to the rule, where some data can be collected without prior consent in specific situations. Even though this was done in order to make things easier and prevent abuses, it has faced some criticisms.

However, the passage of the Digital Personal Data Protection Act, 2023 marks definite progress towards creating regulatory structures for the handling of personal data in India. This is the outcome of an attempt to create a balance between innovation and principles through regulation.

4. Rights of Data Principals under the Digital Personal Data Protection Act

To begin with, the Digital Personal Data Protection Act, 2023 creates a comprehensive legal framework in India for ensuring the protection of informational privacy of the citizens through establishing various rights, which will be vested in the individuals referred to as data principals.

[23] Digital Personal Data Protection Act 2023.

These rights seek to enhance transparency, accountability, and fairness during the processing of personal data carried out by both public authorities as well as corporations. Granting such individual rights in the new legal framework conforms to the constitutional recognition of the right to privacy under Article 21 of the Indian Constitution after the landmark judgment of Justice K.S. Puttaswamy v. Union of India (2017).

In addition, one of the important rights provided in the proposed legal framework is the right to obtain personal data. Under this right, individuals have a legal right to obtain all relevant information regarding the kinds of personal data collected, purposes of processing personal data, and the identity of the data fiduciary handling personal data. This, in turn, makes it possible to ensure transparency during the processing of personal data.

One more protection afforded by the Act involves the right of an individual to ask for correction or updating of his/her personal data where such data is inaccurate. Given that erroneous personal information may be grounds for denying the person services, damage to reputation, and even administrative mistakes, having the right to update such information becomes critical. In addition, people are accorded the right to request for deletion of personal data which is no longer needed for any specific purposes of collection. Thus, personal information will not be stored unnecessarily.

Lastly, the Act affords individuals the right to revoke consent given for processing personal data. Such provision serves to reinforce the concept of information self-determination as individuals will continue to have control over their personal information. Re-voking consent guarantees that processing personal data will always require an affirmative choice on the part of the data principal.

Apart from these rights, the Act grants individuals the right to make use of grievance redressal systems in instances where there is misuse or any processing of personal data that is done without proper authority. Individuals can address their grievances to data fiduciaries and even have their claims heard by the Data Protection Board of India[24], if necessary. Having such a system of grievance redressal helps enforce statutory rights as well.

[24] Digital Personal Data Protection Act 2023, ch V.

These rights being recognized under the Digital Personal Data Protection Act, 2023 indicate the intent of the law to empower individuals in the realm of digitization and ensure that any processing of personal data is done as per the principles enshrined in our Constitution.

5. Duties of Data Fiduciaries under the Digital Personal Data Protection Act

The Digital Personal Data Protection Act of 2023 sets out a series of obligations for data fiduciaries regarding the management of personal data. The purpose of such obligations is to create conditions in which personal data is used in accordance with the rights of privacy and personal freedom enshrined in the Constitution, as well as to facilitate efficient digital governance and commerce. Therefore, the Act attempts to find the right balance between protecting the rights of individuals and creating effective digital systems.

The main obligation that data fiduciaries must adhere to when processing personal data involves its use only for specific reasons related to consent from the data principal or a legal justification for such processing. In other words, such a requirement means that personal data can be processed for legitimate purposes only after the consent from the data principal is provided. Such obligation ensures transparency in the processing of personal data.

The Digital Personal Data Protection Act 2023 ensures adequate protection to privacy in India by defining individual rights, called as data principals' rights, which guarantee that their personal data is used fairly, transparently, and in an accountable way by both public institutions as well as organizations. This provision of the act is congruent with the principle that the right to privacy is a basic legal right under Article 21 of the Constitution as decided in Justice K.S. Puttaswamy v. Union of India 2017.

For clarity, the act provides individuals the right to access details regarding processing of their personal data by any entity. When individuals decide to invoke such a right, they can learn about kinds of personal data being processed and how

6. Role of the Data Protection Board of India

According to the Digital Personal Data Protection Act of 2023, the establishment of the Data Protection Board of India is one of the major milestones that will regulate personal data

processing in line with the law. Therefore, this act is a huge leap forward towards the protection of privacy amidst rapid technological developments in India. It is critical to recognize individual privacy rights while at the same time having a regulatory body that is competent enough to monitor compliance as well as resolve any challenges that may be associated with the misuse of personal information.

Under this act, the Data Protection Board of India has been entrusted with several significant duties. First, the board can receive and process complaints on illegal data processing by data fiduciaries. Whenever there is a violation of the regulations, individuals are expected to report to the board regarding their concerns about the misuse of their personal information. The board has jurisdiction to investigate such complaints and determine whether the Act has been violated. In essence, this grievance system forms an integral part of asserting individual rights.

The other important function performed by the Board is to ensure compliance with the requirements imposed on data fiduciaries. The Board may issue directives that compel the organization to take remedial action against any violation of the requirements set forth under law. Furthermore, it enjoys the power to impose penalties on those who fail to comply with the rules pertaining to the lawful processing of data, security, and breach notifications.

7. Government Exemptions under the Digital Personal Data Protection Act

The Digital Personal Data Protection Act, 2023 acknowledges that the right to privacy cannot be absolute and can be restricted by the State in accordance with its interests relating to national security, sovereignty and integrity of the country, maintenance of public order, and prevention and investigation of offences. To facilitate the proper discharge of their duties in these respects, the Act also contains certain provisions granting exemptions from the requirement to obtain the consent of the data principal for processing his personal data under certain conditions. The need for these exemptions arises from the practical consideration of making it possible for the agencies of government to perform their roles without any restrictions imposed by the privacy rules.

The agencies of the government require access to digital information for various purposes, including gathering intelligence, combating cyber-crimes, maintaining law and order, and implementing welfare schemes involving verification of identities and eligibility of the

recipients of the benefits. The exemptions granted by the Act make it possible for them to do so in cases where such processing is essential for them to discharge their duties.

On the other hand, the extent of the exemptions accorded to the government authorities has elicited significant controversy among legal experts. The apprehension is that wide discretionary powers for personal data processing may compromise informational privacy protections if not guided by sufficient procedural checks. Given that surveillance operations typically entail gathering and evaluating private information, the lack of an autonomous oversight structure may allow for the abuse of these powers.

In the case of Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court stressed that any curtailment of privacy rights must comply with the constitutionally mandated criteria of legality, necessity, and proportionality. According to these conditions, restrictions imposed on privacy rights must be founded in law, pursue a justifiable aim, and maintain proportionality to the nature of the menace posed. Consequently, exemptions granted under the Digital Personal Data Protection Act should conform to constitutional constraints and must be complemented by proper safeguards guaranteeing transparency and accountability.

Effective judicial scrutiny and periodic evaluation of these surveillance techniques would help maintain the right balance between the demands of national security and safeguarding the rights to privacy of the individual citizen. Maintaining a proper balance is critical to making sure that the exceptions made through this Act do not infringe upon the constitutional principles of informational privacy in India.

8. Challenges in Implementation of Data Protection Laws in India

Though the Digital Personal Data Protection Act, 2023 has been passed into law, there still exist certain practical difficulties involved in the process of ensuring its proper implementation in India. The ability to enforce data protection rules effectively cannot be seen as dependent merely on awareness about statutory rights of individuals. On the contrary, it requires that all relevant organizations possess adequate capacity and capability to deal with legal obligations. In the case of the contemporary Indian scenario, an accelerated development of systems of digital governance and the widespread use of digital communication have resulted in many difficulties in the process of monitoring such compliance in numerous government and non-government organizations.

A crucial problem associated with implementation of the Digital Personal Data Protection Act involves the need to provide sufficient institutional capacity to regulatory authorities for proper enforcement of the Act's provisions. As is known, the responsibilities of the newly established Data Protection Board of India will include dealing with complaints regarding the violation of privacy of citizens due to unauthorized use of their personal information. Therefore, providing trained professionals with technical expertise in data protection and cybersecurity is extremely important.

Another significant issue that needs to be addressed pertains to insufficient public knowledge about their rights and duties with regard to data protection. It is necessary to recognize the fact that numerous people fail to realize the extent to which they can protect themselves from having their private data misused by utilizing available resources within the current law. Encouraging digital literacy and informing people about their privacy rights would become instrumental in improving the effectiveness of the regulatory system.

The fact that digital communications do not respect geographical boundaries raises an issue concerning how the process of enforcing data protection regulations would proceed. This issue arises because protecting personal data would be difficult without international cooperation and harmonization of existing laws.

It has also been pointed out that there may be certain issues related to extensive exemptions provided to government bodies and necessity for improving procedures in order to ensure greater transparency. It is especially critical to increase supervision of activities associated with surveillance of digital traffic.

Solutions to such problems through institutional capacity building and creating awareness among the citizens as well as formulating proper regulatory frameworks will be essential for proper implementation of data protection legislation in India, thereby ensuring a proper balance between the two aspects.

CHAPTER 4

CONFLICT BETWEEN NATIONAL SECURITY AND INDIVIDUAL PRIVACY

1. Concept of National Security and Individual Privacy

The other two vital interests in any constitutional democracy include national security and individual privacy. Whereas national security is the need for the State to ensure that it adopts all necessary measures to guarantee the security of the country from internal and external attacks, individual privacy is the need for the State to protect individual liberties, which are protected under the Constitution. In the contemporary world, there has been a growing tension between individual privacy and national security owing to the development of technology and its impact on electronic surveillance tools adopted by the government.

National security can be defined as the responsibility of the government to ensure that it takes all measures to protect the nation from all forms of threats ranging from terrorism, cyber-attacks, espionage to organized criminal groups. To discharge this responsibility, the government has to undertake intelligence operations to identify any threats and then use modern technology to monitor communication networks as well as intercept information electronically.

However, the use of the power of surveillance poses certain questions related to the protection of the right to privacy of citizens. Privacy is directly linked to personal freedom and dignity recognized under Article 21 of the Constitution. In the landmark judgment of Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court, in recognizing the right to privacy as a fundamental right, stressed that citizens should be protected from any arbitrary interference with their private life and correspondence by the state agencies. It was observed that the privacy right allows the development of a person's personality and exercise of other freedoms enshrined in Part III of the Constitution without being subjected to unnecessary interference.

In conclusion, there is a direct connection between the right to privacy and national security which implies the necessity to find a balance between the interests of the state and the protection of individual rights. Although the implementation of surveillance programs is necessary to ensure public security and protect citizens from criminal activities, an

inappropriate infringement on personal data could lead to a violation of democratic principles and constitutional freedoms.

In the present-day digital era, this act of balance has become even more difficult because of the dependence on computerized communication and digital governance systems that deal with a large amount of personal data. The maintenance of the constitutional boundaries in the functioning of surveillance systems and also the effective safeguarding of national security is a major issue that confronts modern democracies like India.

2. Surveillance Framework in India

The legislation governing the use of the surveillance technology in India has been provided in several statutory laws such as The Indian Telegraph Act, 1885[25] and Information Technology Act, 2000 that give the power to government agencies to intercept and decrypt messages under certain circumstances in the interest of national security and public order. The need to have these provisions in these legislations arises due to the responsibility of the State in keeping the country stable internally while also protecting the country from any acts that might pose a threat to the sovereignty and integrity of the country.

For instance, Section 5(2) of The Indian Telegraph Act, 1885 gives the government the power to intercept messages in case there is a public emergency and public safety concerns. It is one of those provisions that have been commonly relied upon by governments in regulating telephone interception and other forms of telecommunication interception with regard to national security matters. Even though this Act was formulated during colonial rule, it continues to be important today in regulating communications surveillance technology.

Like this, Section 69[26] of the Information Technology Act, 2000 allows for the issuing of directions by the Central and State Governments for the interception, monitoring, or decryption of information generated, transmitted, received, stored, or controlled through any computer resource. This power is allowed wherever deemed necessary in the interest of protection of sovereignty and integrity of India, defence of the country, security of the state, public order, and prevention, detection, investigation, or prosecution of an offence. This shows the

[25] Indian Telegraph Act 1885, s 5(2).

[26] Information Technology Act 2000, s 69.

understanding of the relevance of digital surveillance in response to new security challenges due to developments in technology.

Nevertheless, the wide scope of the powers of surveillance vested in these sections has led to apprehensions about inadequate measures of independent oversight in the process of interception and monitoring of communication. In fact, critics have opined that the lack of proper procedures might lead to the abuse of such surveillance powers and violation of individual informational privacy.

Taking into account these considerations, the Supreme Court has in various rulings reiterated that any kind of surveillance activity needs to be in conformity with the constitutionally required principles of legality, necessity, and proportionality. Thus, transparency and accountability in the use of the powers of surveillance becomes crucial for the proper balancing of the requirements of national security with individual liberties in India's digital governance architecture.

3. Section 69 of the Information Technology Act, 2000 and Digital Surveillance

Section 69 of the Information Technology Act, 2000 represents one of the most significant statutory provisions governing digital surveillance in India. The provision authorizes the Central Government and State Governments to intercept, monitor, or decrypt information generated, transmitted, received, or stored in any computer resource where such action is considered necessary in the interest of sovereignty and integrity of India, defence of the country, security of the State, maintenance of public order, or prevention and investigation of offences. With the rapid expansion of digital communication technologies, this provision has become increasingly important in enabling law enforcement agencies to respond effectively to emerging threats such as cybercrime, terrorism, online radicalization, and digital espionage.

In the contemporary digital environment, communication increasingly takes place through electronic platforms such as email services, social media networks, instant messaging applications, and cloud-based storage systems. These platforms generate large volumes of personal data that may be relevant for intelligence gathering and crime prevention activities. Section 69 provides statutory authority for accessing such information when necessary for protecting national security and maintaining public safety. The provision therefore plays a

crucial role in enabling the State to respond to technological changes affecting the nature of security threats in modern society.

However, use of the powers of surveillance under Section 69 poses several challenges concerning the protection of informational privacy. As interception and monitoring entail the gathering of private information from individuals, there is always the risk that exercising such powers could lead to an infringement on the right of individual freedom without proper measures put in place to protect against such occurrences. The lack of judicial oversight prior to interception was noted as an issue that needed attention in relation to constitutional protection of privacy.

The Supreme Court of India in Justice K.S. Puttaswamy v. Union of India (2017) highlighted the criteria for the imposition of restrictions on privacy. These criteria include legality, necessity, and proportionality. According to the criteria for restricting privacy, surveillance should have legal backing, should aim at protecting a legitimate interest, and should not be more extensive than necessary in addressing the risk. This implies that use of interception under Section 69 should be exercised in accordance with constitutional boundaries.

4. Surveillance Provisions under the Indian Telegraph Act, 1885

The Indian Telegraph Act, 1885 is one of the oldest statutes on the interception of communications in India. Even though it was formulated at a time when India was under colonial rule mainly to ensure that telegraph services were regulated, it continues to be relevant in contemporary times in the context of regulation of the surveillance of communication systems. Under Section 5(2), the Government of India may intercept any message when there is an occurrence of any situation of public emergency or any threat to public safety and such interception is necessary for ensuring that the sovereignty and integrity of India, security of the State, and public order are maintained.

The right of the State to intercept communications provided by Section 5(2) has been extensively used to regulate the surveillance of telephone and other telecommunication services. As a result of advancements in technology and emergence of new types of threats in society such as terrorism and organized crime, this provision has become even more significant.

It ensures that potential threats are detected in advance and steps are taken to prevent the commission of any criminal activity which can affect public safety.

Nevertheless, questions have been raised regarding the language of Section 5(2) of the Act, as well as the potential abuse of surveillance powers in the absence of adequate procedural safeguards. Given that the Act predates the advent of digital communication technologies, the measures prescribed under the Act fail to cater to the issues arising out of surveillance technologies equipped with the ability to gather extensive amounts of personal data

.

Considering the same, in People's Union for Civil Liberties v. Union of India (1997), the Supreme Court laid down comprehensive guidelines regulating telephone tapping, underscoring the need for interception of communication to be carried out in strict compliance with the provisions of law. In this regard, the Court mandated that all interceptions be approved by authorized agencies, as well as subject to regular reviews in order to ensure that there is no arbitrary abuse of surveillance powers.

In light of the present-day digital revolution, there is an increased awareness regarding the necessity for reforming the laws related to surveillance in a manner consistent with the constitutional framework.

5. Role of Intelligence Agencies in Ensuring National Security

ntelligence agencies have a major contribution towards securing the national security interests by way of information gathering, analysis, and dissemination relating to possible threats that can affect the sovereignty, safety, and stability of the nation. Given the present state of security challenges like terrorism, cyber-attacks, foreign intelligence espionage, and organized crime, there is a need for proper handling of the same through intelligence and advanced technology. Therefore, the use of surveillance technologies to monitor communications as well as analyze digital information is a common feature in modern-day intelligence operations.

In India, there are intelligence agencies like the Intelligence Bureau and Research and Analysis Wing that contribute to internal and external security concerns respectively. It is necessary to use the services of intelligence agencies in order to determine any security threats in form of extremism and terrorism from abroad as well as cyber-terrorism. Information provided by the intelligence agencies contributes to the timely action by the law enforcement authorities.

However, the working of intelligence agencies requires extensive data to be collected and processed concerning persons. As intelligence services operate in an exclusive manner on account of national security considerations, their monitoring and reviewing by the general public remains very difficult. Such an approach gives rise to apprehensions about surveillance measures adversely impacting the informational privacy rights of the people.

The ruling of the Supreme Court of India in the case of Justice K.S. Puttaswamy v. Union of India, 2017 concerning privacy as a fundamental right has added constitutional protection against any excess in the surveillance measures adopted by the intelligence agencies. The court has pointed out that surveillance must follow legality, necessity, and proportionality for it to fit into constitutional provisions protecting personal liberties.

It is important for intelligence operations to have proper mechanisms for overseeing its activities to restore public trust in national security institutions. Parliamentary, judicial, and internal controls can play a vital role in this regard and ensure proper coordination between constitutional and national security considerations.

6. Issues of Mass Surveillance and Privacy Concerns

Mass surveillance is defined as the process through which the State, with the help of technology including electronic communication networks, digital data banks, biometrics and internet, monitors the personal information of its citizens. In the age of new digital technologies, it is possible for states around the world to use more sophisticated means of mass surveillance in order to gather information from their citizens about various aspects of their lives related to security, crime prevention and order-maintenance. While such a practice might be highly beneficial in terms of building strong security regimes, there are many issues related to privacy rights and democracy that arise as well.

Within the context of India, the advent of new digital government policies, including those using Aadhaar system and other methods of online service delivery, has helped in increasing the amount of personal information collected by the government. While this helps to improve governmental efficiency and enhance service delivery, it might pose dangers if proper safety measures are not taken into account. Mass surveillance without appropriate safeguards can mean an encroachment upon individual freedom protected by the Constitution.

Another problem with the practice of mass surveillance is that there is usually little or no transparency about how the system operates. The reason for this is that surveillance operations take place in secrecy because of national security issues, making citizens unaware of how much of their personal information is being collected or analyzed by State agencies. Lack of transparency will lead to a lack of trust in digital systems of governance, with uncertainty surrounding the issue of safeguarding fundamental rights.

It was held in Justice K.S. Puttaswamy v. Union of India (2017), that privacy is a very important aspect of personal freedom guaranteed by Article 21 of the Constitution. Privacy cannot be violated without the surveillance measures fulfilling the principles of legality, necessity, and proportionality. The three requirements will limit any surveillance actions so that they do not go beyond the necessary extent for serving the legitimate objectives of the State.

In order to strike a balance between the interests of national security and privacy rights of an individual, it is necessary to ensure transparency, accountability, and oversight into the operation of surveillance systems. This can be done by ensuring sufficient legal regulation of the collecting and processing of private data.

7. Doctrine of Proportionality in Privacy Restrictions

In constitutional analysis, the principle of proportionality occupies the most pivotal position in deciding the issue of constitutional legality in connection with the restriction of basic human rights, including the right to privacy. The essence of the principle is that all restrictions of individual liberties should be made in connection with pursuing the legitimate purpose of the state, and should be proportionate and necessary. This rule ensures that the State actions that limit individual freedom are justified as much as possible for ensuring national security or public peace.

The significance of the principle of proportionality as a constitutional requirement can be traced in the case of Justice K.S. Puttaswamy v. Union of India (2017). The Supreme Court recognized in its decision that any infringement on privacy can take place only on condition of meeting several conditions. Firstly, it should be made in accordance with laws adopted in a certain case. Secondly, the purpose of such interference should be connected with ensuring the safety of

national security or committing crime. Finally, the means used should be proportional to the purpose pursued.

In light of this, the application of the doctrine of proportionality in cases related to digital surveillance becomes extremely important since modern technologies make it possible to collect huge amounts of information about people. Otherwise, without necessary limits, any surveillance techniques used can lead to serious violations of human freedom and can pose a threat to democracy guaranteed to citizens by the Constitution. As such, the proportionality principle becomes an effective mechanism for measuring whether a measure introduced by the State for the sake of national security is justified or not.

The importance of the proportionality doctrine lies also in its significance as one of the most powerful mechanisms of judicial review of various surveillance activities performed by the State. This way, the principle enables the Court to assess whether certain restrictions introduced by the State are reasonable and necessary and, thus, to find a proper balance between two equally important interests – national security and human freedom.

8. Judicial Approach toward Surveillance Powers in India

The approach adopted by judiciary with respect to the surveillance powers is extremely important as it helps regulate the powers of State authorities and ensure that those powers are used within the purview of the Constitution of India. As surveillance powers relate to accessing personal information and communications, they are likely to violate the right to informational privacy recognized under Article 21 of the Constitution. Therefore, there was an urgent need to adopt judicial intervention in order to regulate and ensure proper implementation of these surveillance powers.

An early example of judicial intervention in this regard could be observed in People's Union for Civil Liberties v. Union of India (1997). In the present case, the constitutionality of telephone tapping under the Indian Telegraph Act, 1885 was challenged before the Supreme Court. The court observed that telephone tapping is an infringement of right to privacy and it should be done only in accordance with law. Several guidelines were formulated for interception which include obtaining authorization from concerned authorities and regular review of interception orders.

In the historic decision in the case of Justice K.S. Puttaswamy vs Union of India (2017), the judicial recognition of the right to privacy was extended even further. The court ruled that privacy is a fundamental right that is an integral part of the right to life and personal liberty under Article 21. It further provided that any measure of surveillance on personal data must comply with certain standards of legality, necessity, and proportionality.

This decision highlights the fact that judicial pronouncements concerning surveillance powers take into account the need to strike a balance between the needs of the State for national security purposes and the need to safeguard the liberty of the individual in a democracy.

Such judicial decisions continue to serve the important function of ensuring that surveillance measures comply with constitutional norms while at the same time allowing the State to discharge its duty of protecting national security in the digital era.

CHAPTER 5

COMPARATIVE ANALYSIS OF DATA PRIVACY LAWS IN OTHER COUNTRIES

1. Data Protection Framework under the European Union's General Data Protection Regulation (GDPR)

Firstly, it can be mentioned that the General Data Protection Regulation[27], adopted in 2016 and implemented starting from 2018 by the European Union, is one of the most progressive frameworks for regulating protection of personal data in the current age of digitization. Such framework introduces a unified standard across all the countries of the European Union and creates the legal environment which guarantees the effective protection of informational privacy. At that, it follows a rights-based approach which is associated with the recognition of such values as individual freedom and self-determination of the subjects.

One of the key provisions established by the GDPR concerns the lawful nature of collection and processing of the personal data. According to the mentioned regulation, such procedures may take place only upon the condition that the person provides his or her explicit and informed consent. As a result, such an approach is beneficial for informational self-determination because individuals have a right to withdraw their consent and control the use of the data provided.

GDPR also lays down a number of crucial principles concerning the processing of personal data, such as purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. The principle of purpose limitation stipulates that data must be collected for specific, lawful purposes and can be stored for the duration that is sufficient to achieve them. The principle of accountability demands that appropriate measures for protecting personal data must be implemented by all organizations dealing with such data.

One more key element of GDPR is that extensive rights of the data subjects are acknowledged. The right to access personal data, the right to data rectification, the right to restriction of processing, the right to data portability, and the right to object to the processing of personal data are among these rights. Perhaps the most important right granted to data subjects by the

[27] Regulation (EU) 2016/679 (General Data Protection Regulation).

regulation is the right to be forgotten, according to which personal data can be deleted from databases if it is no longer needed or justified.

Furthermore, the GDPR creates supervisory authorities that are independent in each member state to ensure compliance with GDPR and penalize any violation of this regulation. Supervisory authorities have considerable power to penalize entities that fail to adhere to standards concerning data protection by subjecting such entities to hefty fines. Such strong regulatory structures have been vital in ensuring that privacy safeguards are effectively implemented within the EU.

Consequently, the GDPR is a critical example when developing data protection regimes within other jurisdictions, especially India. Issues of transparency, accountability, and enforcement mechanisms can guide nations in developing robust informational privacy regimes without compromising on security concerns.

2. Data Privacy Framework in the United States

In contrast to the European Union, there is no single unified system of legislation regarding personal information protection in the United States. The US has a sector-based model for regulation of the issue at hand, whereby various types of personal information are governed by different legislative acts that regulate the respective industries. This model stems from the history of the development of privacy legislation in the United States and the need to balance individuals' privacy interests with the interests of innovation and national security.

There are a number of key pieces of legislation regulating protection of personal information in the United States on a sector-by-sector basis. For example, the Health Insurance Portability and Accountability Act[28] regulates handling of medical data by medical institutions and health insurance providers. The same applies to the Gramm-Leach-Bliley Act[29] that addresses issues related to collection and use of financial data by banks. Finally, the Children's Online Privacy Protection Act[30] provides certain safeguards regarding collection of personal data of minors on the Internet.

The Federal Trade Commission is one of the institutions that ensure consumer privacy in the U.S. The agency regulates companies that indulge in unfair and misleading data practices. It

[28] Health Insurance Portability and Accountability Act 1996 (US).

[29] Gramm-Leach-Bliley Act 1999 (US).

[30] Children's Online Privacy Protection Act 1998 (US).

enforces privacy policies in organizations to ensure compliance. As such, the FTC relies heavily on institutional enforcement mechanisms to regulate privacy as opposed to legislative frameworks.

On the other hand, the issue of consumer privacy in the U.S. is shaped largely by national security laws such as the Patriot Act[31] and Foreign Intelligence Surveillance Act[32]. These laws allow the tracking of communication that concerns anti-terrorism efforts and national security issues. Despite the usefulness of these surveillance measures in enhancing security, they have been associated with debates on informational privacy and civil liberties issues.

Although the US does not have a comprehensive legislative instrument such as the GDPR, it has nevertheless managed to create effective institutions aimed at mitigating any cyber threats and safeguarding consumer interests in cyberspace. The case of the US shows that privacy protection is attainable by means of sectoral laws, regulations, and legal checks and balances.

3. Data Protection Law in the United Kingdom

A complete and effective legal framework to protect personal data has been put into place in the United Kingdom with the help of the Data Protection Act, 2018[33], which is accompanied by the UK GDPR. Even though the UK has formally left the European Union due to Brexit, it still maintained a data protection regime similar to the one created under the European Union General Data Protection Regulation. This indicates that the UK has not compromised its privacy protections and has also tried to make sure that any transfers of personal data across borders is facilitated without any hindrances.

As per the provisions of the Data Protection Act, 2018, there are certain guidelines laid down for collecting personal information by authorities, whether they are public bodies or private enterprises. All such processing activities related to personal data are required to be conducted in a manner that is lawful and is also done keeping transparency in mind

Another critical characteristic of the UK data protection system is that it recognizes extensive rights of individuals whose personal data is processed. Individuals have the right to access personal data, the right to rectify inaccurate data, the right to restrict the processing of personal

[31] USA PATRIOT Act 2001 (US).

[32] Foreign Intelligence Surveillance Act 1978 (US).

[33] Data Protection Act 2018 (UK).

data, and the right to object to the processing of personal data when the processing affects their interests. Individuals also have the right to request the deletion of personal information if it is no longer required for the purpose of collection.

The UK has put in place an independent regulatory body known as the Information Commissioner's Office (ICO). The ICO is responsible for ensuring that organizations comply with the UK data protection law and privacy protections. The ICO has extensive investigatory and enforcement powers, including the ability to levy fines against organizations that do not comply with their statutory obligations regarding the protection of personal data. The existence of an independent regulatory body greatly enhances public trust in privacy regulation.

Apart from securing personal data within national jurisdiction, the legal regime of the United Kingdom also governs the cross-border transmission of personal data in order to make sure that any such cross-border activity takes place when there is sufficient protection for the data being transferred. It is thus evident how vital it is to be in harmony with international standards of privacy in the present-day interconnected digital world. Such lessons learned from the United Kingdom can serve as a useful template for designing institutions in India.

4. Lessons for India from International Data Protection Frameworks

Comparative study of international data protection regimes would shed some light on the improvement of India's legislative approach to regulate personal data processing in the digital era. As the sphere of digital governance widens and the number of people relying on communication via internet increases, it becomes crucial for India to develop the regulatory measures that will ensure both informational privacy and national security and economic needs of the country. The experience of EU countries, the US, and the UK can be applied to the problem under discussion to achieve this goal.

The most significant lesson to be learned from the GDPR legislation is the importance of creating a reliable enforcement mechanism that includes the role of independent supervisory authorities to monitor data protection compliance. The effectiveness of the mentioned regulation results from the existence of such entities that have the authority to penalize companies violating the provisions of the law with substantial financial penalties. Thus, it can be stated that enhancing institutional independence of the DPAI will considerably strengthen the process of enforcing privacy rights in India.

Yet another valuable insight concerns the need for comprehensive individual rights over personal information. The GDPR regime illustrates the significance of ensuring empowerment of individuals by means of rights to access, rectification, restriction of processing, and erasure of personal data. Including such rights in India's regulatory regime would result in increased accountability in digital governance.

The US's adoption of a sectoral approach to regulation reflects the need to adopt a specialized regulatory framework for personal information falling under sensitive categories such as health care information, financial information, and children's information. Adopting such measures in the Indian context could lead to enhanced protection of vulnerable types of personal data.

The case of the United Kingdom also highlights the significance of the independence of regulatory supervision and compatibility with international laws concerning the transfer of personal information across borders. With India's growing involvement in global digital business processes, compatibility with international data protection regulations will become necessary to foster economic collaboration and ensure safe transfer of data across borders.

As such, a comparative study shows that an effective strategy for safeguarding informational privacy involves creating a well-balanced regulatory system based on institutional autonomy, strict enforcement, and acknowledgment of individual rights. Integrating such principles into India's developing data protection system will prove vital for achieving equilibrium among technological development, security concerns, and fundamental rights in the digital world.

CHAPTER 6

FINDINGS, SUGGESTIONS AND CONCLUSION

1. Findings of the Study

This paper explores the legal framework for the protection of personal data in India against the backdrop of fast-developing technologies and increasing utilization of digital governance. An important conclusion made from the research findings is that the decision of the Supreme Court of India recognizing privacy as a fundamental right guaranteed by Article 21 of the Constitution in Justice K.S. Puttaswamy v. Union of India (2017) marks an unprecedented shift in constitutional law in India. It improved the level of protection of informational privacy and created a constitutional basis for regulation of processing and collection of personal data by state and non-state entities.

Moreover, the research found that before the introduction of the Digital Personal Data Protection Act, 2023 in India, there was no comprehensive legislation aimed at regulating processing of personal data in a digital environment. While some provisions of the Information Technology Act, 2000 and Information Technology Rules, 2011 regulated the processing of sensitive personal information, these provisions were rather restrictive and did not fully cover the issues associated with processing of large amounts of data in digital governance systems.

In addition, another major finding from the study is that although the Digital Personal Data Protection Act offers important protections through rights of data principals and responsibilities of data fiduciaries, questions have been raised about the independence of the Data Protection Board of India as well as the exemptions provided to government agencies when dealing with personal data in matters relating to national security and public order. This raises issues related to the ongoing balance between privacy protection on the one hand and the State's interest in security on the other.

An important aspect of the discussion on privacy is the issue of surveillance and the relevant laws in India, particularly the Indian Telegraph Act, 1885, and the Information Technology Act, 2000. While both these acts play an important role in ensuring that intelligence agencies can deal with security threats, there is evidence from the study to suggest that they need updating so as to align them with constitutional protections of informational privacy.

Comparative study of various global legal frameworks including EU's GDPR, U.S. sectoral approach to privacy legislation, and the UK data protection system indicates that the effectiveness of personal data protection depends on having robust enforcement measures and the presence of autonomous regulatory bodies. This implies the need to enhance institutional measures in India's data protection system in order to provide adequate privacy protection without compromising national security.

2. Suggestions of the Study

The following steps can be undertaken to improve the protection of personal information in India along with the effective implementation of constitutional provisions regarding informational privacy. Firstly, one of the main suggestions that arise from this research paper is that efforts must be made to strengthen the independence and effectiveness of operations of the Data Protection Board of India. As the success of any regulatory regime hinges upon the credibility and independence of its enforcement apparatus, increasing the independence of this institution will definitely contribute towards increased compliance with laws enacted under the Digital Personal Data Protection Act, 2023.

Secondly, an issue which requires special attention is that of the extent of exemptions which have been provided for government organizations under the Digital Personal Data Protection Act. Even though these exemptions have been incorporated to enable effective functioning of intelligence agencies and law enforcement bodies with respect to the maintenance of national security and crime prevention, there must be proper procedural guarantees which prevent arbitrary intrusions upon individual liberty rights. Increased judicial supervision over acts of surveillance will definitely facilitate maintaining a proper balance between these laws and constitutionally guaranteed freedoms..

Furthermore, it is recommended that laws related to surveillance, like the Indian Telegraph Act of 1885, and certain provisions of the Information Technology Act of 2000, should be revised and modified so that they are in line with current advancements in technology as well as with the constitutional standards for safeguarding the privacy of information. This will aid in the creation of clear protocols for monitoring communications and make surveillance activities accountable.

It is also imperative that people become aware of their right to data protection and the provisions in the laws which protect them. People lack knowledge about these provisions due to which they are unable to have any sort of control over their information. Awareness campaigns can play an important role in improving the efficacy of the data protection system in India.

Additionally, incorporating best practices such as the GDPR from the European Union, which involves stronger processing of personal data based on consent and increased accountability standards, would facilitate greater transparency in digital governance mechanisms. By incorporating these measures, India will be able to build an effective balance between privacy and technology, thereby achieving its regulatory, innovation, and security goals.

3. Conclusion of the Study

The exponential growth in technology has completely revolutionized the process of gathering, analyzing, and storing personal data not only by government agencies but also by private bodies. While digital governance has enabled greater efficiency in the provision of services and provided people access to economic opportunities, it has also brought with it several difficulties, including those of protecting the right to informational privacy and preventing any misuse of personal data. In such circumstances, the constitutional recognition of the right to privacy as a basic right guaranteed under Article 21 of the Constitution is one of the most important milestones in the history of Indian constitutional law. The seminal decision in K.S. Puttaswamy v. Union of India (2017) laid down the constitutional framework for regulating the processing of personal data and ensuring that privacy will remain an indispensable part of personal freedom.

The introduction of the Digital Personal Data Protection Act, 2023 is a positive step towards the development of a comprehensive statutory framework that regulates the processing of personal data in India. Through the identification of the right of individuals and the obligation of organizations dealing with personal data, the law makes a significant contribution to enhancing informational privacy in the digital governance framework. Yet, it is essential to enhance institutional structures that will ensure the implementation of statutory provisions and the transparency of surveillance powers.

Additionally, the importance of maintaining a balanced approach concerning the relationship between the need for surveillance for national security and the right to privacy must be

emphasized. Surveillance tools employed by agencies for the purpose of addressing potential threats to national security should comply with constitutional norms and be subject to judicial review to avoid the abuse of power associated with the use of personal information. Comparative assessment of foreign legislation shows that the protection of informational privacy requires the existence of independent regulatory authorities, effective enforcement tools, and the broad recognition of rights to personal data.

In conclusion it is thus clear that the protection of privacy in the modern world necessitates the formulation of a proper legal framework based on constitutional protections, robust regulatory structures, judicial scrutiny, and public knowledge. This would make it possible for India to promote technological growth as part of its overall development efforts without compromising on democracy or individual dignity.