NATIONAL SECURITY SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: CONSTITUTIONAL LIMITS AFTER THE PUTTASWAMY JUDGMENT

***SHRUTI MUDGAL**

ABSTRACT

The recent boom in digital technologies has greatly expanded the ability of governments to collect, process, and analyses personal information to serve as a tool of governance, law enforcement, and national security. Although the surveillance systems are frequently justified as the necessary measures to keep the order in the society and safeguard the interests of the nation, they also cause severe concerns on the issue of privacy of individuals and informational independence. The justice system acknowledging privacy as a fundamental right in Justice K. S. Puttaswamy v. in India. Union of India was a ground breaking case in constitutional jurisprudence because it introduced a case law that tests of legality, necessity, and proportionality had to be met in limiting the right to privacy. The Microsoft Digital Personal Data Protection Act, 2023 is the first major law in India regarding the processing of digital personal data. Among the key concepts that have been proposed in the Act are the principle of data principals, data fiduciaries, data processing based on consent, and regulatory supervision in the form of the Data Protection Board of India. But there are also huge exemptions of government agencies in the Act, especially under Section 17 that permits the State to handle personal data in the name of national security, sovereignty and order. The study analyzes the issue of whether the existing data protection framework as defined in the Digital Personal Data Protection Act protects the constitutional right to privacy and at the same time permits the State to fulfill any genuine national security interest. The study makes use of a doctrinal approach of legal research method to analyses the constitutional principles, statutory laws, judicial precedents and the literature on privacy and surveillance in the Indian context. The paper contends that despite the Digital Personal Data Protection Act being an important contribution to the regulation of personal data processing, extensive exemptions granted to state authorities

*LL.M., Gujarat National Law University – Silvassa Campus

are likely to undermine privacy rights unsupported by effective oversight, transparency, and accountability systems. The study finds out that a balance between national security and individual privacy is achieved by enhanced procedural guarantees and better clarity of legal standards to ensure that surveillance practices do not override constitutional guarantees in the digital era.

Keywords: Privacy; Digital Personal Data Protection Act; Surveillance; National Security; Data Protection; Constitutional Law.

INTRODUCTION

The swift growth of digital technologies has contributed greatly to the increased capacity of governments to gather, store and analyses personal information to govern, enforce the law and assure national security. Digital monitoring, communicating through interception, and data analytics are all becoming the surveillance systems that can be employed to resolve such threats as cybercrime, terrorism, and other security threats. Although these measures can be required to preserve the national interests, they also bring up significant concerns on the issue of preserving the privacy of individuals and informational autonomy. In India, the traditional legal framework governing surveillance has largely been derived from the **Indian Telegraph Act, 1885** and the **Information Technology Act, 2000**, which grant the State powers to intercept communications and monitor digital information for security purposes[1].

In India, the constitutional environment concerning privacy has undergone a major change due to the historic ruling in the Justice K. S. Puttaswamy v. case. In Union of India, the right to privacy was unanimously recognised by the Supreme Court as a fundamental right in Article 21 of the Constitution[2]. The Court held that privacy is intrinsic to human dignity, personal liberty, and individual autonomy[3]. Notably, the decision held that any limitation on the right to privacy should pass the constitutional test of legality, necessity, proportionality as well as provision of sufficient procedural protection[4]. These principles have become central in evaluating the validity of state surveillance measures in India.

[1] Indian Telegraph Act, 1885, §5(2); Information Technology Act, 2000, §69 (India).
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[3] Ibid 3–4 (per Chandrachud J.)
[4] Ibid180–182

In response to the increasing importance of regulating personal data in the digital age, India enacted the **Digital Personal Data Protection Act, 2023**, which provides a statutory framework governing the processing of digital personal data by both private entities and public authorities[5]. The Act introduces key concepts such as data principals, data fiduciaries, consent-based data processing, accountability obligations, and regulatory oversight through the Data Protection Board of India[6]. The legislation seeks to protect informational privacy while facilitating lawful data processing in a rapidly evolving digital ecosystem.

However, the Act also contains significant exemptions for government agencies under Section 17, which permit the State to process personal data in the interests of national security, sovereignty, public order, and other related grounds[7]. These exemptions raise important constitutional concerns, particularly regarding whether such broad powers are consistent with the privacy protections recognized in the Puttaswamy judgment. The possibility of extensive state access to personal data without strong oversight mechanisms may create risks of excessive surveillance and potential misuse of personal information.

In this context, the present research examines the constitutional limits of national security surveillance in India in the post-Puttaswamy era, with particular reference to the **Digital Personal Data Protection Act, 2023**. The study analyses whether the legal framework established under the Act adequately balances the legitimate interests of national security with the protection of the fundamental right to privacy in a constitutional democracy.

LITERATURE REVIEW

1. *Privacy and Surveillance Conflict: A Comparative Analysis of the laws in the USA and India* (Vaibhav Chadha et al., 2022- This Paper Privacy and Surveillance Conflict examines how the two biggest democracies strike a compromise between the necessity of surveillance and the right to privacy. It emphasizes how both India and the US acknowledge privacy as a fundamental value despite having different sociopolitical environments, yet they frequently give priority to national security when surveillance is warranted[8]. The authors deliver a

[5] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
[6] Ibid. s2, 6, 8, 27.
[7] Ibid s17
[8] Chadha, V., Balasubramanian, T., & Bhuwalka, A. (2022). Privacy and Surveillance Conflict: A Comparative Analysis of the laws in the USA and India. *JANUS NET e-journal of International*

comparative overview of surveillance laws in both jurisdictions, showing that the problem between liberty and security is a recurring theme across democracies.

It does not go into great detail about India's constitutional structure following the Puttaswamy ruling, even if it is successful in pointing out the similarities and differences between the USA and India. In particular, it does not examine how India's surveillance regulations relate to the proportionality concept, which mandates that monitoring techniques be legitimate, necessary, and reasonable.

Also, the research does not examine how constitutional protections are in comparison to other Indian regulatory regimes such as the Telegraph Act, Information Technology Act, surveillance architectures like NATGRID and CMS. Furthermore, it does not examine government studies (e.g., the report of the Justice B. N. Srikrishna Committee) and judicial pronouncements that are required to understand the shifting landscape of privacy in India.

2. *Privacy & National Security: A Balancing Act?* by Divyanshu Dembi (2021)

It examines the inherent contradiction in safeguarding national security and safeguarding individual privacy. It highlights the issue of governments often justifying surveillance practices in the name of security, whereas civil liberty campaigners and people in general stress the significance of preserving privacy as a fundamental right.[9]

Finding a balance between these conflicting interests is one of the most important issues of the digital age, as this paper emphasizes in its context of democratic governance. The paper does not provide a thorough doctrinal analysis of how constitutional guarantees are implemented in various jurisdictions, especially in India after the Puttaswamy ruling, even though it recognizes the problem between privacy and national security. The paper does not examine whether India's surveillance laws, such as the Telegraph Act, Information Technology Act, or technologies such as the Central Monitoring System and NATGRID, meet the standard of proportionality set by the Supreme Court. Additionally, it does not incorporate case commentary or government studies that are essential to comprehending the changing constitutional framework, like the Justice B. N. Srikrishna Committee Report

Relation.

[9] Dembi, D. (2021). Privacy & National Security: A Balancing Act?. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3953357.

3. *National Security vs Privacy in India* by Aneesha A. Kharpor (2021)

In the modern era, privacy and national security have taken center stage. National security is the defense and protection of a nation's citizens, whereas privacy is one of the fundamental human rights that is essential to maintaining human dignity. However, the increasing test of strength between citizen privacy and national security has once again brought up the question of where a fine line of balance exists between the two. The advancement in the technological world has made it viable for the Government to collect data and store hundreds of data points about an individual[10]. The viability has further reduced the position of the individual's privacy. The article analyses the concept of an individual's privacy in India and its appraised link with national security. The article also discusses the various facets of privacy and national security. The article also takes the views of the citizens of the country regarding the altercation between national security and privacy.

4. *Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns* by Debasish Nandy (2023)

The paper discusses the challenges that have arisen due to the rapid growth of surveillance technology, which are affecting the protection of human rights. The challenges are related to the violation of privacy, breach of data, and the abuse of power by governments and corporations for surveillance purposes.[11] The issues are also discussed in the context of international debates, with reference to legal and ethical frameworks, case studies, and international approaches to balancing national security interests with human rights to privacy, freedom of expression, freedom of assembly, etc.

***5. Balancing Security and Liberty: Examining Contemporary Counterterrorism Laws* by Ali Masyhar et al. (2023)**

The paper examines the complex issue of striking a balance between the imperatives of national security and the protection of civil liberties in the context of modern counter-terrorism legislation. In this respect, the paper contextualizes the analysis in the wake of the threat of global terrorism, where many countries across the globe have enacted significant legislation to

[10] Kharpor, A. (2021). National Security vs Privacy in India. Spectrum: Humanities, Social Sciences and Management.
[11] Nandy, D. (2023). Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns. Journal of Current Social and Political Issues

combat the threat of terrorism. However, these procedures sometimes raises concerns about infringements on privacy rights, due process, and broader civil liberties[12]. The research critically examines new frameworks in countering terror attacks, considering their implications for democratic values and personal freedoms. The research is guided by various case studies from different jurisdictions, where there are instances of surveillance, information sharing, and technology affecting already disadvantaged groups. The study is also noteworthy for its assessment of oversight structures and legal scrutiny of counter-terror measures. It also discusses the role of international cooperation and technology in forming current counterterrorism efforts.

Ultimately, Furthermore, the paper suggests that a balanced approach to the issue is necessary to ensure that security is not compromised while the basic rights and liberties that are the hallmark of democratic countries are not infringed upon. The paper adds to the discourse by stressing the need for a responsible approach to counterterror measures that respect the rights of individuals.

6. Dynamics of Liberty and Rights in Crisis – State, National Security and Individual Rights

(2025)

The paper seeks to address the intricate relationship between the state and national security and how such a relationship affects an individual's rights. The paper suggests that in protecting a country's national security, the state compromises an individual's liberties in the name of the greater good. The relationship between the state and an individual's liberties can be described as a tripartite relationship.[13] The study examines the history of the scope of national security and its effect on rights, with a comparative analysis from different countries. The significance of the study lies in its advocacy for the balance between national security requirements and the rights of individuals, without compromising the rights for the sake of national security.

7. A Study of Pegasus Snooping Case: Is it a Matter of National Security or Individual Right to Privacy **by Utkarsh Yadav (2024)**

In the paper, the controversy surrounding the Pegasus spyware scandal in India is discussed,

[12] Ali Masyhar et al. (2023)
[13] (2025). Dynamics of Liberty and Rights in Crisis - State, National Security and Individual Rights. International Journal of Research and Scientific Innovation.

along with how the use of military-grade spyware for targeted surveillance of journalists, lawyers, government officials, opposition politicians, and activists raised constitutional concerns. The paper locates the debate in the larger conflict between national security concerns and the fundamental right to privacy, mentioning the recognition of the fundamental right to privacy by the Indian Supreme Court in K.S. Puttaswamy v. Union of India (2017)[14]. It addresses issues of policy and judicial determinations, aiming to examine the construction of privacy and security in India.

8. *The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance* by J. Mavedzenge (2020)

The article focuses on the way governments in Africa are dealing with national security threats through the use of communications surveillance. The impact on the right to privacy is also discussed[15]. The article highlights that surveillance is done under the name of security, which impacts the right to privacy. The right to privacy has to be protected under the principle of proportionality. The paper posits that privacy is just as important as the protection of national security, and it challenges the notion that prior judicial authorization is the only means for ensuring proportionality. It seeks alternative means and mechanisms that have been put in place by some African countries for authorization of surveillance in a bid to balance individual rights and security concerns.

9. *Shielding Privacy in the Surveillance Era* by Stency Mariya Mark et al. (2024)

The article discusses the violation of the right to privacy on the basis of national security. It presents a comparative analysis of the development of the human right to privacy in India, South Africa, and the US. It has used judgment analysis to conclude that the protection afforded by the law on privacy is much higher in South Africa than in India and the US; India ranks second in the order[16]. The paper also discusses how revelations such as the Pegasus case in India and the Snowden case in the US have shown the weakness of privacy protection.

[14] Yadav, U. (2024). A Study of Pegasus Snooping Case is a Matter of National Security or Individual Right to Privacy. International Journal of Science and Research (IJSR).
[15] Mavedzenge, J. (2020). The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance. African Journal of Legal Studies, 12, 360-390.
[16] Mark, S., & Pandey, A. (2024). Shielding Privacy in the Surveillance Era. Law, State and Telecommunications Review.

Significantly, the authors have proposed the idea of "silencing surveillance," where surveillance is not just carried out to provide security but to silence voices of dissent. In essence, it highlights the debate on a global scale regarding whether privacy trumps utilitarianism in the state, cautioning against arbitrary access to personal data in the name of national security that threatens fundamental rights. It does so by adding to the debate by putting Indian privacy law in a comparative context and cautioning against the threat of surveillance in a democratic country.

10. Limiting of the Right to Privacy in the Context of Protection of National Security by B. Praneviciene (2011)

The paper describes how some natural rights, such as privacy and secrecy in communication, are being curtailed in the name of securing the nation. The paper describes how the conventional understanding of the concept of security is mainly centered on securing the state from external threats such as aggression, invasion of boundaries, and attacks on institutions, while assuming that human rights protection will be taken care of. The paper highlights that a secure state does not mean that the citizens in that state are secure since curtailment of human rights in the name of securing the state can be a threat to the citizens[17]. In fact, the article highlights this, showing how national security can compromise some of the most fundamental human rights, such as the right to privacy. In a sense, what the study does is highlight the compromise between national security and human rights, arguing that while national security is a fundamental requirement for a state's existence, it is a compromise on personal freedoms. In fact, it argues that privacy is one of those human rights that is most compromised in a bid for national security, raising concerns about how far a state can go in compromising personal freedoms in a bid for national security.

11. National Security, Personal Privacy and the Law by Sybil Sharpe (2019)

The book examines the dynamic relationship between surveillance practices, national security, and individual privacy in the context of recent significant disclosures like the Snowden affair and the Cambridge scandal[18]. The book also emphasizes the impact of these disclosures on the public perception of surveillance practices. The book also explores issues of increasing convergence between intelligence agencies and police powers, which have given cause for concerns over unauthorized surveillance and its encroachment on freedom of association and

[17] Praneviciene, B. (2011). Limiting of the right to privacy in the context of protection of national security. , 1609-1622.
[18] Sharpe, S. (2019). National Security, Personal Privacy and the Law.

expression. Sharp discusses recent legal reforms designed to mitigate the risks of unauthorized electronic surveillance and offers insight into how this balance between security measures and individual liberty is addressed under the social contract. The work also challenges the assumption that individuals consent to a loss of privacy through their use of social media and online commerce. Finally, there is the question of how this fits in with the overall debate over state surveillance. The book can be characterized as a critical re-evaluation of the debate between national security and privacy.

12. ***Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance*** **(2018) by Francesca Bignami**

The chapter discusses the international law perspective on the issue of the right to privacy regarding the activities of spy agencies. The author is particularly concerned with the question of whether U.S. or European law offers any kind of "extra-territorial" protection for the right to privacy[19]. The author discusses U.S. law, noting that it makes a "sharp distinction between insiders (citizens/permanent residents) and outsiders," granting much stronger protections to insiders while limiting protections for foreigners. The author also discusses the EU perspective, noting that while the EU does not have internal jurisdiction over its own spy agencies, it does have agreements with the U.S. regarding the access of foreigners to EU personal data. However, the European Court of Human Rights has jurisdiction over European spy agencies. The case law of the ECtHR indicates that it would likely hold that European agencies must respect privacy rights whenever they exert control over personal data, even when that control is extraterritorial. The chapter generally emphasizes the current patchwork of privacy protection in the face of national security surveillance, as it contrasts the insider-outsider dichotomy of the U.S. approach with the expansive, albeit limited, approach to extraterritorial privacy rights in Europe.

13. ***National Security, Surveillance, and Human Rights*** **by Christakis Théodore et al. (2021)**

In this article, the connection between national security issues, surveillance measures, and human rights protection will be discussed. It has already been recognized that restrictive measures in the name of national security are included in international law as "adjustment variables" for human rights law[20]. However, the chapter cautions that these mechanisms are

[19] Bignami, F., & Resta, G. (2018). Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance. , 357-380.
[20] Christakis Théodore et al. (2021)

often abused by governments and security agencies, being used as a means to monitor political opponents, suppress dissent, or hide misconduct.

The authors emphasize that in a democratic society, surveillance must be balanced against the freedoms enjoyed by the public, especially that of privacy.

In order to explain this point further, the chapter will discuss the case law from the European Court of Human Rights (ECtHR) and identify three key criteria that the ECtHR employs in order to determine if the law on surveillance is compliant with the European Convention on Human Rights. In essence, the chapter will focus on the need for surveillance, as well as the risks that it poses, and argue that the misuse of "national security" provisions threatens the rule of law and democratic principles.

14. Pratyay Panigrahi and Eishan Mehta (*The Impact of the Puttaswamy Judgement on Law*, NUJS Law Review, 2022)

The paper discusses the implications of the Supreme Court's landmark judgment on the Puttaswamy case, which identified the fundamental right to privacy. The paper starts with an overview of the dichotomy between the need to control crime (efficiency in detecting and controlling crime) and the need to ensure due process (fairness, checks, and rights[21]). The authors identify the antecedents in pre-Puttaswamy jurisprudence from M.P. Sharma (1954) and Kathi Kalu Oghad (1961), which recognized extensive state powers in search and seizure, to Gobind (1975), PUCL (1997), and Canara Bank (2005), which recognized privacy concerns and developed procedural checks. The authors identify the development in the courts' recognition of privacy as an inherent component of Article 21 before its formal constitutionalization and then examine the decision in Puttaswamy itself in relation to the antecedents in pre-Puttaswamy jurisprudence and offer some comparative insights from the U.S., South Africa, and Canada. It contends that search provisions are particularly susceptible to challenges to privacy where procedural protection is weak and suggests that a rigorous proportionality test is to be used to determine the constitutional validity of the provisions. Finally, the authors explain how existing provisions of search under the CrPC, Income Tax Act, NDPS Act, MCOCA, etc., need to be examined in the context of the Puttaswamy judgment.

15. **Government Surveillance vs. Privacy Rights: Examining Exemptions in the DPDPA**

This paper *Examining Exemptions in the DPDPA* critiques Section 17 of the DPDPA (2023), showing how its broad exemptions for government agencies undermine privacy protections by

[21] Pratyay Panigrahi and Eishan Mehta , NUJS Law Review, 2022.

not only permit surveillance without judicial safeguards, proportionality checks or accountability, but also place the Indian system in the context of international best practices, such as the GDPR in the EU and the FISA in the U.S., which show that India is closer to an autocratic than a democratic system. Some of the risks highlighted in the paper include chilling effects on free speech, function creep, and destruction of public trust, with reforms including judicial tribunals, transparency reporting, increased independence of the Data Protection Board and sunset clauses.

CASE COMMENTARY

JUSTICE K S PUTTASWAMY (RETD.), AND ANR. v. UNION OF INDIA AND ORS. (Writ Petition (Civil) No. 494 of 2012) AUGUST 24, 2017

This judgment was a constitutional landmark, as a nine-judge bench of the SC unanimously held that the right to privacy was a fundamental right under Article 21[22], overruling the precedents of M.P. Sharma (1954) and Kharak Singh (1962), which had denied the right to privacy. The opinion of Justice D.Y. Chandrachud was also based on the fact that "privacy is a natural and inalienable right intrinsic to liberty and dignity," which also includes "informational privacy against surveillance and misuse of personal data" in the digital age. The Court also held that "any limitation placed on the right to privacy must meet the test of proportionality," while also upholding Justice Subba Rao's dissenting judgment in Kharak Singh that "arbitrary surveillance infringes personal liberty." The judgment also placed privacy within comparative constitutional law (UK, US, SA, Canada, ECtHR), thereby reshaping Indian constitutional law to assess surveillance laws and counter-terror laws to ensure that national security does not override privacy. Citation: Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, per Chandrachud J.

GOVERNMENT REPORTS

Justice A.P. Shah Committee Report (2012)[23] – Privacy Framework

[22] Gn, P. (2023). Justice K. S. Puttaswamy (RETD) VS. Union of India & ORS. SSRN Electronic Journal.
[23] Shah Report (2012)

This was India's first attempt at outlining a framework on privacy. It proposed National Privacy Principles based on international norms (OECD & EU) and highlighted the importance of transparency, accountability, and monitoring in surveillance by the State. The committee cautioned against any arbitrary invasion of the private lives of citizens, particularly in the context of Aadhaar, NATGRID, and DNA profiling.

National Cyber Security Policy (2013)[24]

The policy sought to create a secure and strong cyberspace for citizens, enterprises, and the government. The mission of the policy was to secure critical information infrastructure, minimize vulnerabilities, and address cyber threats through collaborative mechanisms. The policy was centered on national security but failed to address privacy issues for individuals.

TRAI Consultation Papers on Data Privacy (2017–2018)[25]

TRAI consultations focused on aspects of privacy, security, and ownership of telecom users' data. The consultations concluded that the existing laws (Information Technology Act, Telegraph Act, etc.) were not sufficient for the digital landscape. The consultations recommended that users own their data, with greater accountability for telecom service providers. There was a recommendation for sectoral regulation, which is consistent with the overall data protection framework .

Justice B.N. Srikrishna Committee Report (2018)[26] – Data Protection

In the footsteps of Puttaswamy, this committee drafted India’s first comprehensive data protection framework. It suggested the concept of a fiduciary relationship between individuals (data principals) and entities (data fiduciaries), focusing on consent and accountability. It also suggested a Data Protection Authority for enforcement.

[24] Cyber Security Policy (2013)
[25] TRAI Papers (2017–18)
[26] Srikrishna Report (2018)

RESEARCH GAP

Although existing literature highlights the issue of national security surveillance and privacy in India, the majority of the literature focuses only on the Indian Telegraph Act, 1885, and the Information Technology Act, 2000. However, not much research has been done on the Digital Personal Data Protection Act, 2023, in particular, in terms of the exemptions granted to the government in comparison to the privacy guidelines set in the case of Justice K. S. Puttaswamy v. Union of India.

RESEARCH PROBLEM

The increased use of digital surveillance technology by governments worldwide has raised a number of concerns over the protection of individual rights to privacy. In India, the existing laws on surveillance were framed before the advent of modern digital communication technology. Examining whether these regulations adhere to constitutional principles guiding privacy constraints becomes vital once privacy is acknowledged as a basic right.

OBJECTIVE

1. To identify the constitutional position of the right of privacy in India.
2. To analyse the legal framework that governs security surveillance in India.
3. To evaluate whether existing laws regulating security surveillance are in conformity with the proportionality test set by the Supreme Court of India.
4. To suggest some recommendations on how legal provisions that safeguard privacy can be enhanced.

RESEARCH QUESTIONS

1. Whether the recognition of the right to privacy in Justice K.S. Puttaswamy v. Union of India establishes any restrictions on national security surveillance in India.
2. Whether the Indian Telegraph Act of 1885 and the Information Technology Act of 2000 provisions on surveillance are constitutional under the proportionality test.
3. Whether India's system of surveillance strikes a balance between national security concerns and the right to privacy

SCOPE AND LIMITATIONS

This paper will analyse the constitutional and legal framework that regulates national security surveillance and privacy in India, specifically in the context of the Digital Personal Data Protection Act, 2023 and its interface with the Information Technology Act, 2000, in the context of the principles laid down in the case of Justice K. S. Puttaswamy v. Union of India. This paper will use a doctrinal methodology, but it is purely a legal analysis and does not involve any empirical study, and the fact that the DPDPA is a new law means that many of its provisions, especially those involving exemptions by the government, are untested in the courts.

METHODLOGY

The methodology for conducting the research will be a doctrinal legal research methodology. This involves conducting a study on constitutional provisions, statutory laws, and academic literature on privacy and surveillance. The primary sources for the study will be legislation and case laws, while the secondary sources will include books, research articles, journal publications, and government publications. This will help in evaluating whether existing surveillance laws are constitutional or not.

MAIN COMPONENTS

The recognition of the right to privacy by the Constitution in the Puttaswamy judgment has resulted in a revolutionary shift in the law relating to privacy in India. The Court held that “Privacy is an essential facet of personal liberty and human dignity.” Significantly, the judgment has for the first time in India incorporated the principle of proportionality as a constitutional principle for determining state interference in the right to privacy.

According to this theory, surveillance methods need to meet three important criteria. First, the restriction needs to have a solid legal foundation that has been created by legislation. Second, the action must aim to achieve a justifiable state goal, such crime prevention or national security. Third, there must be precautions against abuse and the interference must be proportionate to the goal being pursued.

Nevertheless, several issues remain in regard to the application of this doctrine in existing surveillance laws in India. The Telegraph Act and Information Technology Act have given wide powers to government agencies to carry out interception of communication, but these acts do

not have proper oversight mechanisms with judicial authorization in several cases.

In addition to this, the development of surveillance systems like NATGRID and the Central Monitoring System has given rise to further concerns about transparency. It is because these systems allow for the analysis of huge amounts of digital data, which could have a major impact on individual privacy if not properly regulated.

Legal Framework of Data Protection under the DPDPA

The Digital Personal Data Protection Act, 2023 is a statutory regulation of the collection, processing, and storage of digital personal data in India. The Act provides several fundamental principles which are aimed at making sure that personal information is used in a legal, open and responsible way.

The Act constitutes people as data principals and data processing entities as data fiduciaries thus maintaining a fiduciary relationship that places duty on the data fiduciaries to be responsible when handling personal data. The Act further demands that personal information should be handled on the basis of free, informed and specific consent of the information principal except in a few legitimate purposes as stipulated in the Act.

Also, the Act provides the formation of the Data Protection Board of India as a regulatory organ that would control the adherence to the rules, resolve complaints, and punish in the case of violation of the data protection duties.

Nevertheless, another of the most controversial issues of the Act is the exemptions of government agencies. According to Section 17 of the Digital Personal Data Protection Act, the Central Government can provide certain exemptions to its instrumentalities with the view of sovereignty, integrity of India, security of the State, friendly relations with the foreign States, and preservation of the public order.

Such exemptions bring about the issue of protection of sufficient checks to prevent overbearing state surveillance. Although national security is a valid goal of the State, constitutional jurisprudence developed in the Puttaswamy case stipulates that any privacy limitation should meet the proportionality test.

So, the issue of the compatibility of such exemptions with the constitutional privacy protection remains a burning question in the emerging Indian data protection framework**.**

CONCLUSION

Increasing speed of technological changes has significantly enhanced surveillance of the contemporary state and, therefore, the conflict between the national security and the privacy protection. Tension took a constitutional look in India following the historic ruling of the Supreme Court in the case of Justice K. S. Puttaswamy v. Union of India, in which the court said that the right to privacy was a basic right in Article 21 of the Constitution. The decision made it apparent that any restriction of privacy ought to be in accordance with the constitutional tenets of legality, necessity, proportionality, and procedural assurance. These ideals have taken the place of being the yardstick to evaluate the legitimacy of state surveillance practices. Despite this constitutional framework, the current legal framework of surveillance in India remains reliant on previous legislation like the Indian Telegraph Act, 1885 and the Information Technology Act, 2000, which gravel much authority of interception and monitoring to the state. The laws were passed under technological grounds that are far apart to the modern online digital world and thus do not have sufficient procedural protection and transparency measures and external controls. Of such importance in this respect is the enactment of the Digital Personal Data Protection Act, 2023, which is a linchpin move towards the regulation of the processing digital personal data in India. The Act introduces the notions of data principals, data fiduciaries, consented data processing, and filtering mechanism of Data Protection Board of India. Nevertheless, the overall exemptions that Section 17 offers to the public bodies are highly worrisome to the constitution. The exemptions state that the State shall be exemption to the requirements of other individuals regarding the processing of personal data to national security, sovereignty and order. Constitutionally speaking, the existence of such blanket exemptions has cast the appropriateness of such exemptions in relation to the proportionality test as first declared in the Puttaswamy ruling. Even though national security is a valid and essential goal of the State, the absence of solid mechanisms in this respect can potentially result in the threat of facilitating an excess of surveillance and, therefore, jeopardize the defense of informational privacy. In such a way, this research concludes that although the Digital Personal Data Protection Act, 2023 may be considered a significant step in the evolution of the law on data protection in India, it should be ensured that this legislation is accepted and applied in a way that does not conflict with the constitutional right to privacy. It should be noted that the supervising mechanisms should be enhanced and the surveillance should be transparent. Eventually, a balance has to be maintained to ensure that the security measures and the technical advancement does not compromise the basic freedoms, which are the foundation of the constitutional

democracy in India.

BIBLIOGRAPHY

Books

- Solove, Daniel J., *Understanding Privacy* (Harvard University Press, 2008).
- Sharpe, Sybil, *National Security, Personal Privacy and the Law* (Routledge, 2019).
- Westin, Alan F., *Privacy and Freedom* (Atheneum, 1967).

Journal Articles

- Chadha, Vaibhav, T. Balasubramanian & A. Bhuwalka, "Privacy and Surveillance Conflict: A Comparative Analysis of the Laws in the USA and India," *JANUS NET e-journal of International Relations* (2022).
- Dembi, Divyanshu, "Privacy & National Security: A Balancing Act?" *SSRN Electronic Journal* (2021).
- Kharpor, Aneesha A., "National Security vs Privacy in India," *Spectrum: Humanities, Social Sciences and Management* (2021).
- Mark, Stency Mariya & A. Pandey, "Shielding Privacy in the Surveillance Era," *Law, State and Telecommunications Review* (2024).
- Mavedzenge, J., "The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance," *African Journal of Legal Studies* (2020).
- Nandy, Debasish, "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns," *Journal of Current Social and Political Issues* (2023).
- Panigrahi, Pratyay & Eishan Mehta, "The Impact of the Puttaswamy Judgement on Law," *NUJS Law Review* (2022).
- Prashant, Pragya. *Government Surveillance vs. Privacy Rights: Examining Exemptions in the DPDPA*. Chandigarh University, 13 Aug. 2025.

- Yadav, Utkarsh, "A Study of Pegasus Snooping Case: Is it a Matter of National Security or Individual Right to Privacy," *International Journal of Science and Research* (2024).

Government Reports

Justice A.P. Shah Committee Report on Privacy.

- National Cyber Security Policy.
- TRAI Consultation Papers on Data Privacy.
- Justice B.N. Srikrishna Committee Report on Data Protection.

Cases

- Justice K. S. Puttaswamy v. Union of India.