THE DIGITAL PANOPTICON AND ARTICLE 21: RE-EVALUATING THE RIGHT TO PRIVACY IN INDIA'S DATA-DRIVEN CONSTITUTIONAL MORALITY

Chethan D Malled, BBA LLB, MKPM RV Institute of Legal Studies[1]

ABSTRACT

The Right to Privacy, recognized as an inherent part of the "Right to Life and personal Liberty" under Article 21 of the Indian Constitution by the Supreme Court in the pivotal K.S.Puttaswamy vs Union of India judgment, is currently facing an unprecedented modern challenge. My research examines how the mass collection of personal data by both the government and large corporations is creating a pervasive, subtle surveillance environment—what I term the "Digital Panopticon." This constant threat of being monitored—even when one isn't actively being watched—is forcing citizens to change their behaviour, thereby eroding the core principles of autonomy and dignity that underpin the Constitution.

This paper critically analyses the country's protective measures, particularly the effectiveness of the new Digital Personal Data Protection Act (DPDPA), 2023. While this legislation fulfils the legal mandate for a data law, its numerous and expansive exemptions for government agencies—often based on vague grounds like 'public order' or 'national security'—are deeply problematic. I argue that these broad exceptions undermine the constitutional guarantees, creating a significant tension with Constitutional Morality—the requirement that the spirit of the Constitution must always be prioritized over administrative convenience.

To prevent the fundamental right to privacy from becoming merely symbolic, the judiciary must re-evaluate its role. I recommend that the courts enforce a much stricter standard of proportionality, compelling the State to prove that its intrusive data collection methods are absolutely necessary and minimally invasive. Ultimately, the survival of India's commitment to justice and liberty in the digital age depends on the courts actively defending the private lives of its citizens against the unchecked power of the data-driven State.

Keywords: Digital Spying, Privacy Rights, Government Data Access, Constitutional Rules, Article 21, Supreme Court Verdict, New Data Law, Proportionality Test.

[1] BBA LLB, MKPM RVILS, (KSLU), Bangalore

Chapter 1: Introduction

The right to privacy, as guaranteed by **Article 21** of the Indian Constitution, has evolved as a pillar of personal liberty and human dignity in the digital age. The momentous decision in *Justice K.S. Puttaswamy v. Union of India* (2017) altered India's constitutional landscape by recognizing privacy as a basic right inherent in life and liberty.[2] The Supreme Court underlined that privacy protects autonomy, informational control, and freedom from unjustified government intervention. However, the advent of data-driven governance has created a new paradigm known as the **Digital Panopticon**, in which residents are continually monitored via digital footprints, biometric identification, and algorithmic profiling.[3]

This widespread surveillance, facilitated by technology such as **Aadhaar**, **CCTV networks**, and **artificial intelligence**, has blurred the line between human freedom and state efficiency, raising serious concerns about consent, autonomy, and responsibility.[4]The **Digital Personal Data Protection Act of 2023 (DPDPA)** aims to institutionalize privacy protection, but detractors contend that it also legitimizes widespread state and corporate data surveillance.[5] This study aims to answer the essential question: *Does the DPDPA truly protect privacy, or does it mainstream a surveillance culture under the pretence of digital governance?* The study's goal is to examine the tension between technology governance and constitutional morality in modern India.

Chapter 2: Conceptual Framework — The Digital Panopticon and Privacy

The *Panopticon* is a building design created by **Jeremy Bentham** in the 18th century, where a single observer can watch all inmates without them knowing when they are being observed.[6] This constant possibility of surveillance makes people self-regulate their behaviour, creating an automatic system of control.[7] India's expanding metadata surveillance—fueled by *Aadhaar* linkages, telecom data-retention rules and apps like *Aarogya Setu*—has created a digital

[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[3] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York: Vintage Books, 1977) — introducing the concept of the Panopticon as a model of surveillance and power.
[4]Reetika Khera, "Aadhaar and the Infrastructural Power of the State," *Economic and Political Weekly* 54, no. 15 (2019): 36–43.
[5] Internet Freedom Foundation (IFF), "India's Digital Panopticon: Privacy and Surveillance in the DPDP Act, 2023," *Policy Brief* (2023).
[6]Jeremy Bentham, *Panopticon; or, The Inspection-House* (London: T. Payne, 1791).
[7] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York: Vintage Books, 1977).

panopticon that chills dissent, endangers journalists and marginalised groups, and reshapes democracy. The **Digital Personal Data Protection Act, 2023** grants data rights and a regulator but allows broad government exemptions and weak oversight.[8] Surveillance technologies have evolved from traditional observation to advanced digital systems like CCTV, drones, biometrics, and AI-driven analytics. While these enhance crime prevention, national security, and public safety, they raise serious ethical and privacy concerns. Governments worldwide employ programmes such as **PRISM**, **Tempora**, **Echelon**, **SORM**, and India's **CMS** for monitoring communications, often criticised for overreach and human rights violations.[9] Future surveillance integrating AI, IoT, and biometrics demands ethical AI development, transparency, and updated legal safeguards. Without these, surveillance risks eroding democracy and fundamental human rights, as affirmed by the Supreme Court in the *Puttaswamy* judgment recognising privacy as intrinsic to dignity and liberty.[10]

Chapter 3: Constitutional and Legal Framework of Privacy in India

In India, the right to privacy has evolved over time through judicial interpretation. Initially, cases such as *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962) denied the constitutional right to privacy.[11] However, successive decisions broadened the reach of Article 21 to include human liberty and dignity. The turning point was *Justice K.S. Puttaswamy v. Union of India* (2017), in which a nine-judge bench unanimously declared privacy a fundamental right under Article 21, safeguarding autonomy, personal data, and informational privacy in the digital age.[12]

LandmarkJudgment:

Justice K.S. Puttaswamy v. Union of India (2017) — The Supreme Court held that the Right to Privacy is intrinsic to the Right to Life and Personal Liberty under Article 21, affirming it as a fundamental right and establishing principles of consent, proportionality, and data protection in modern governance. Further, the Supreme Court identified three key components of privacy — autonomy, dignity, and informational privacy. Autonomy ensures individuals' freedom to

[8] Ministry of Electronics and Information Technology (MeitY), *Digital Personal Data Protection Act, 2023*, Government of India.
[9] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014)
[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[11] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300; *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[12] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

make personal decisions about their body, identity, and life without external interference. Dignity upholds the inherent worth of every individual, recognizing privacy as essential for self-respect and human development. Informational privacy protects control over personal data, preventing unauthorized collection, storage, or dissemination of information. Together, these principles form the foundation of the constitutional right to privacy under Article 21, linking it to liberty, equality, and personal freedom in the digital era.[13]

The relationship between **Article 19(1)(a)** and **Article 21** demonstrates the balance of free expression and personal autonomy. Article 19(1)(a) guarantees the freedom to express and access information, but Article 21 defends dignity, privacy, and autonomy. They, along with **Article 14**, create the Constitution's "Golden Triangle." Courts strike a balance between the public's right to know and individuals' right to privacy, guaranteeing proportionality and legality. Constitutional morality directs this balance, prioritizing justice, equality, and dignity over popular feeling. It enables courts to interpret the Constitution as a living text, ensuring that governance is consistent with fundamental rights and moral constitutional ideals.[14]

Chapter 4: The Digital Personal Data Protection Act, 2023 — Promise and Paradox

The **Digital Personal Data Protection Act (DPDPA)** of 2023 is India's first comprehensive data privacy legislation, aimed at protecting personal data in the digital economy. The law's potential resides in establishing a structured framework: it names Data Fiduciaries (those who decide how data is processed) and requires them to get free, explicit, informed, and unambiguous consent from the Data Principal (the individual) before processing personal information. The Act clearly defines important user rights, such as the right to knowledge, correction, and erasure of data. Enforcement is delegated to the **Data Protection Board of India (DPBI)**, which has the authority to impose significant financial penalties for noncompliance.[15]

Despite its progressive architecture, the DPDPA contains a substantial paradox, particularly **Section 17**, which allows the Central Government to exempt its own agencies from the Act's

[13] Ibid. (per Chandrachud, J.) — The Court identified autonomy, dignity, and informational privacy as core facets of the right to privacy.
[14] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 — established the interrelationship between Articles 14, 19, and 21 forming the "Golden Triangle."
[15] Ministry of Electronics and Information Technology (MeitY), *The Digital Personal Data Protection Act, 2023*, Government of India.

restrictions. The grounds for these exemptions, such as "sovereignty, integrity, security of the state," and "public order," are overly vague and wide. This gives the executive branch broad authority to collect and process citizen data without the accountability norms required of private businesses, resulting in a significant, harmful loophole that fundamentally undermines the right to privacy.[16]

Furthermore, there are worries about the system's enforceability and independence. The Data Protection Board's structure, with its appointment and service conditions established by the Central Government, raises severe concerns about its ability to judge impartially against the government and its agencies. Critically, the statute lacks sufficient court monitoring; appeals are routed through the **TDSAT** rather than allowing direct, forceful judicial examination of fundamental rights issues. When compared against worldwide benchmarks such as the **EU's General Data Protection Regulation (GDPR)**, the DPDPA's flaws become more obvious.[17] The GDPR strengthens institutional accountability by establishing an independent supervisory authority and subjecting exemptions to severe necessity and proportionality requirements. Furthermore, the GDPR establishes more expansive rights, such as the express right to data portability.

Finally, while vital and pioneering, the DPDPA is limited by its institutional framework and extensive state exemptions. By putting state privilege ahead of strict checks and balances, the law fails to fully embrace the criteria of constitutional morality, legitimacy, necessity, and proportionality for privacy intrusion demanded by the Supreme Court's landmark **Puttaswamy** ruling.[18]

Chapter 5: Judicial Review and the Role of Proportionality

The **proportionality test**, as definitively adopted by the Supreme Court of India in cases such as *Modern Dental College v. State of Madhya Pradesh* and the seminal *K.S. Puttaswamy v. Union of India* privacy judgment, is a structured judicial mechanism for determining the constitutionality of any state action that restricts a fundamental right.[19] This standard requires that any such restriction be necessary and proportionate, as well as a "culture of justification"

[16]Internet Freedom Foundation (IFF), "Section 17 of the DPDP Act: The Exemption Clause," *Policy Brief* (2023)
[17] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679.
[18] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[19] *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.

from the state. It is composed of four elements: first, the restriction must have a legitimate aim; second, the measure must be suitable to achieve that aim; third, it must be necessary, or the least restrictive means available; and fourth, a proper balancing must be struck, ensuring that the harm to the right is not disproportionate to the public benefit.[20]

The judge must rigorously apply this criterion when reviewing state surveillance programs and the extensive government exemptions included in the **DPDPA**. As the Supreme Court ruled in *Anuradha Bhasin v. Union of India* (2020), restrictions must meet necessity and proportionality standards, particularly the "least restrictive means" test.[21] Groups like the **Internet Freedom Foundation (IFF)** have challenged data collecting programs, stressing how unclear rules threaten mass surveillance, and how a weak application of the proportionality test—particularly its necessity element—can render privacy a "symbolic right."[22]

Chapter 6: The Conflict Between Digital Governance and Constitutional Morality.

Constitutional morality is a dedication to the essential spirit of liberty, equality, and fraternity, which requires the State to prioritize citizens' rights over administrative convenience.[23] In contrast, current digital governance frequently prioritizes immediate efficiency and national security, resulting in a system that systematically ignores consent and accountability. This emphasis on simplifying processes results in extensive data collection and the use of opaque algorithmic decision-making, without giving citizens informed choices or clear paths for redress when violations occur. We see stark examples of this clash in the justification of governmental surveillance—such as the deployment of invasive spyware or ubiquitous facial recognition—on the basis of national security, which severely violates the right to privacy.[24]

This unrestrained digital control weakens democracy in two crucial ways: it suppresses free expression and jeopardizes citizens' autonomy, and it destroys the fundamental trust required for democratic administration by making the government appear more interested in control than service. To uphold constitutional morality, the state must reverse this trend.[25] Every digital

[20] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[21] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[22] Internet Freedom Foundation (IFF), "Proportionality and Surveillance: Evaluating India's Data Privacy Framework," *Policy Brief* (2023).
[23] *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 — The Supreme Court defined constitutional morality as adherence to the values of liberty, equality, and dignity above social or political convenience.
[24] Human Rights Watch, *India: Stop Unchecked State Surveillance* (Report, 2023).
[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 — affirmed privacy as intrinsic to dignity and liberty under Article 21.

incursion into individuals' lives must be subject to rigorous assessment, with justification based on openness and proportionality standards, to ensure that governance tools remain subordinate to the rights they are intended to defend.[26]

Chapter 7: Suggestions and Reforms

Several improvements are required to achieve a balance between privacy and security. First, precise legislative definitions of "national security" and "public order" must be established. Their existing vagueness allows for arbitrary interpretation and manipulation, weakening constitutional rights under Articles 19(1)(a) and 21.

Second, judicial review of nominations and decision-making should be used to strengthen the Data Protection Board's independence and ensure impartial enforcement. Third, enacting a "Right to Data Minimization" will limit data gathering to what is absolutely essential, supporting responsible data governance and lowering abuse risks.

Furthermore, public awareness and digital literacy campaigns must be expanded to inform citizens about their data rights and potential remedies. Citizens who are empowered play an important role in preserving privacy protections.

The privacy-by-design approach should be incorporated into all government technology projects to guarantee privacy precautions are implemented from the start rather than as an afterthought.

Finally, regular judicial audits of surveillance systems should be required to promote transparency, proportionality, and accountability in state surveillance methods.

These reforms would create a rights-based, transparent, and responsible data protection policy, ensuring that technological progress does not come at the expense of individual liberty.

Chapter 8: Conclusion

Privacy is not merely about secrecy; it is about human dignity, autonomy, and freedom—the very essence of personhood. In the constitutional framework of India, privacy safeguards the

[26] B.R. Ambedkar, Constituent Assembly Debates, Vol. VII (1948) — on constitutional morality as the foundation of democratic governance.

individual from the unchecked reach of the State and ensures that liberty remains meaningful in practice. As India advances rapidly in the digital sphere, it must ensure that technological progress does not erode the constitutional soul founded on justice, liberty, and dignity.

Constitutional morality requires the State to act with moral restraint, not merely in legal compliance. Laws and institutions must, therefore, reflect ethical governance, transparency, and respect for fundamental rights. The true test of a democracy lies not in the power it wields, but in the limits it observes.

In the age of the Digital Panopticon, true liberty survives only when privacy remains inviolable—a sacred boundary that upholds the dignity of every individual.

Bibliography / References

Statutes and Constitution:

1. Constitution of India (Articles 19 & 21)
2. Digital Personal Data Protection Act, 2023

Case Laws:

3. K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
4. Anuradha Bhasin v. Union of India (2020) 3 SCC 637
5. Modern Dental College v. State of M.P. (2016) 7 SCC 353
6. Kharak Singh v. State of U.P. (1962) 1 SCR 332
7. M.P. Sharma v. Satish Chandra (1954) SCR 1077

Books & Articles:

8. M.P. Jain, *Indian Constitutional Law* (LexisNexis, 2023)
9. Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* (2016)
10. Soli Sorabjee, "Privacy and the Rule of Law," *SCC Journal*, 2020
11. Pavan Duggal, *Cyber Law in India* (2021)

Reports:

12. Justice B.N. Srikrishna Committee Report (2018)
13. Internet Freedom Foundation (IFF) Policy Reports on DPDPA, 2023

Web Sources:

14. Press Information Bureau, Govt. of India — DPDPA Key Features (2023)