



The Datafied State and Constitutional Privacy - Reconsidering the Limits of Executive Access to Personal Data in India

Dr. Usha Bhonsle¹, Afifa I², Platina K P³, Mukesh MS⁴, HariPriya⁵, Usha⁶, Vinodini⁷

¹Associate Professor, Saveetha School Of Law, ushabhonsle.ssl@saveetha.com

²Scholar, Saveetha School Of Law, 132504127.ssl@saveetha.com

³Scholar, Saveetha School Of Law, Platina12006@gmail.com

⁴Scholar, Saveetha School Of Law, mukeshmaran67@gmail.com

⁵Scholar, Saveetha School Of Law, haripriyamesh808@gmail.com

⁶Scholar, Saveetha School Of Law, usharam3009@gmail.com

⁷Scholar, Saveetha School Of Law, gvinodini2723@gmail.com

Abstract

The expansion of digital governance has transformed the relationship between the Indian State and personal information. Government authorities increasingly collect, store and process identity, financial, biometric, health and behavioural data for welfare administration, taxation, policing and regulatory purposes. While data-driven governance can improve administrative efficiency, it also creates significant constitutional concerns where executive authorities obtain or process personal information beyond the purpose for which it was originally collected. The recognition of privacy as fundamental right under Article 21 has therefore become increasingly significant in determining the limits of State access to personal data. This paper examines the constitutional limitations governing executive access to personal information in India, particularly through the principles of legality, legitimate State purpose, necessity and proportionality. It further examines the Digital Personal Data Protection Act (DPDPA), 2023 and its relationship with constitutional privacy. The paper argues that possession of personal information by the State cannot itself create unrestricted authority to access, combine, analyze or retain that information. A constitutional framework for the datafied State must instead ensure purpose limitation, proportionality, procedural safeguards, accountability and meaningful remedies against unlawful access.

Keywords - Datafied State, Constitutional Privacy, Personal Data, Informational Privacy, Executive Power, Data Protection, Surveillance, Proportionality.

INTRODUCTION

Digitalization has fundamentally altered the manner in which the Indian State interacts with individuals. Government administration increasingly depends upon digital databases containing information relating to identity, residence, taxation, health, welfare benefits, financial transactions and other aspects of individual life. The transition from physical records to interconnected databases has increased administrative efficiency but has simultaneously expanded the State's capacity to observe, analyze and make inferences about individuals. Personal data has consequently acquired significance beyond its immediate informational content. Individual data can possess economic value and can be combined with other datasets to generate further information about a person. The relationship between privacy regulation and value of personal data demonstrates why contemporary privacy protection cannot be confined merely to preventing disclosure of secrets (Canayaz, Kantorovitch & Mihet, 2021). Earlier scholarship concerning India similarly identified the need for stronger legal protection of personal information within India's fragmented privacy framework (Agarwal, 2012).

The constitutional implications are particularly important when the entity accessing personal information is the executive. Government agencies possess powers that private entities generally do not possess, including investigative, regulatory and enforcement powers. Consequently, executive access to personal information may have consequences for individual liberty extending well beyond ordinary commercial data processing. Court's recognition of privacy as a fundamental right, in Justice K.S. Puttaswamy (Retd.) v. Union of India ([2017] 10 SCC 1), established informational privacy as an important constitutional interest. The question today is therefore not simply whether the State can collect personal information, but when and to what extent it can subsequently access, combine, analyze and retain that information.

The DPDPA, 2023 represents an important development in India's statutory framework. Recent scholarship considers the legislation a significant development in India's data-protection regime (Sahoo, 2026). However, statutory regulation operates within the constitutional framework and cannot eliminate the requirement that State interference with privacy satisfy constitutional standards.

THE CHANGING MEANING OF PERSONAL DATA AND PRIVACY

Privacy in the digital environment cannot be understood solely as physical seclusion or secrecy. An individual may voluntarily provide information to a government authority for a particular administrative purpose while nevertheless retaining a legitimate expectation that the information will not subsequently be used for unrelated purposes. The distinction between disclosure and informational control is therefore central. Personal information can remain constitutionally significant even after it has entered government databases. The increasing economic and

administrative value of personal data has intensified this concern (Canayaz, Kantorovitch & Mihet, 2021).

In India, privacy and data protection developed historically through constitutional jurisprudence rather than through a comprehensive data-protection statute. The earlier legal framework consisted of constitutional protections, sectoral legislation and provisions of information technology law (Agarwal, 2012). The position has subsequently developed substantially with the DPDPA, 2023. Recent analysis of Indian data-protection law identifies the DPDPA, 2023 as a major development in India's regulatory framework (Sahoo, 2026). At the same time, recent scholarship continues to examine the changing Indian regulatory environment and implications of developments following the enactment of the legislation (Kumar, Saraf & Singh, 2024; Singh, Inuganti & Sahay, 2026). The problem is particularly significant because digital information can be replicated and shared at virtually no marginal cost. Information collected by one government department may therefore become accessible to another department, creating possibilities of secondary use that were not contemplated at the time of original collection.

CONSTITUTIONAL FOUNDATION OF INFORMATIONAL PRIVACY

The constitutional foundation of informational privacy principally arises from Art. 21, read with the broader guarantees of Part III. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* ([2017] 10 SCC 1), court recognised privacy as a constitutionally protected right encompassing multiple dimensions of individual autonomy and dignity. The recognition of informational privacy is particularly important in the context of State databases. Government possession of information cannot automatically be equated with the absence of a privacy interest. The purpose for which information is collected and circumstances in which it may subsequently be accessed remain constitutionally relevant. The proportionality framework developed in Indian constitutional law requires State interference with fundamental rights to possess a legal basis, pursue a legitimate objective and maintain an appropriate relationship between the means employed and objective pursued.

Recent judicial developments continue to apply privacy principles to technologically mediated forms of information access. In *Dr. Balasubramaniam Rathinavel v. Canara Bank* [2025 SCC OnLine Mad 4835], court discussed informational privacy alongside physical privacy and decisional autonomy. Similarly, in *Hari C.V. v. Indian Institute of Information Technology* [2025 SCC OnLine Ker 4370], court considered the privacy implications surrounding access to personal and professional information under the Right to Information framework. These developments demonstrate that the constitutional protection of privacy does not disappear merely because information is held by a public institution.

The first constitutional limitation on executive access is legality. Where governmental action interferes with privacy, the interference must be supported by law. Administrative convenience or technological capacity cannot constitute a sufficient source of executive authority. This requirement is especially important in relation to data because technological systems can permit government agencies to access information on a scale that may not have been contemplated when the underlying legislation was enacted. The legal authority should therefore identify, expressly or through necessary implication, the circumstances in which personal information may be accessed. A statutory provision permitting information collection for one purpose should not automatically be interpreted as granting unlimited authority for unrelated secondary uses. The requirement of legality also provides a safeguard against executive discretion becoming effectively unlimited. Without a clear legal basis, individuals may have little ability to understand when their information may be accessed or to challenge inappropriate governmental use.

LEGITIMATE STATE PURPOSE AND NECESSITY

A lawful interference with privacy must also pursue a legitimate State objective. Governmental objectives such as preventing crime, protecting national security, administering welfare schemes, enforcing taxation and protecting public health may justify certain forms of data processing. However, the existence of a legitimate purpose does not establish that every form of data access is necessary. For example, an authority investigating financial wrongdoing may legitimately require financial information relating to a particular person. That does not necessarily establish constitutional justification for obtaining unrelated health, communications or location data concerning that person. The requirement of necessity therefore requires the government to demonstrate a rational connection between the information sought and governmental objective. This becomes especially important when large databases are involved. Instead of obtaining information relating to a narrowly defined category of individuals, technological systems may permit authorities to conduct broad searches across entire populations. The constitutional question should consequently focus on whether the same objective could reasonably be achieved through a less intrusive method.

Proportionality is perhaps the most important constitutional limitation on governmental access to personal data. The principle requires consideration of the relationship between the legitimate objective and degree of interference with privacy. In *Chetan Ramniklal Shah v. Union of India* [2024 SCC OnLine Bom 1617], court considered the proportionality of restrictions upon fundamental rights and emphasised the importance of examining less restrictive alternatives. The principle is particularly relevant to digital databases because the scale of possible access can be enormous.

A government agency may technically be capable of accessing millions of records, but technological feasibility cannot by itself establish constitutional necessity. Proportionality should therefore consider the sensitivity of the information; the number of individuals affected; the duration of access; the purpose for which access occurs; the availability of less intrusive alternatives; safeguards governing subsequent use; and mechanisms for review and accountability. Recent scholars similarly emphasizes the importance of privacy-preserving technological mechanisms in the processing of personal information (Park, Oh & Choi, 2023). Technological development can therefore be directed towards reducing unnecessary exposure rather than simply expanding governmental access.

PURPOSE LIMITATION AND FUNCTION CREEP

One of the most significant problems associated with the datafied State is function creep. Function creep occurs where information initially collected for one purpose is subsequently used for another purpose without adequate legal or constitutional justification. For example, information collected for welfare administration may later become relevant to taxation, law enforcement or regulatory investigations. Although each subsequent purpose might independently appear legitimate, the cumulative effect can undermine the individual's ability to understand and control the use of personal information.

Purpose limitation is therefore essential to informational privacy. The problem becomes more complicated where information from different government databases is combined. A person's individual records may reveal relatively limited information, but aggregation can generate a detailed profile. Research on differential privacy illustrates the difficulty of distinguishing personal, anonymous and pseudonymous information in technologically complex environments (Huang & Zheng, 2023). Similarly, research on privacy-preserving identification demonstrates the possibility of designing systems that allow useful processing while reducing unnecessary exposure of personal information (Hwang, Shi & Lee, 2023). Consequently, the constitutional assessment of governmental data access should consider not merely the individual dataset being accessed but also the possibility of combining it with other information.

THE DATA PRIVACY LEGISLATION AND CONSTITUTIONAL PRIVACY

The DPDPA, 2023 provides India's principal statutory framework for digital personal data. Its development represents a shift from India's earlier fragmented approach towards a dedicated legislative regime. Recent scholarship describes the Act as a significant development in India's privacy framework (Saha & Mukhopadhyay, 2024). The legislation must nevertheless be considered alongside constitutional privacy rather than as a substitute for it.

This distinction becomes particularly important in relation to State processing. Constitutional privacy establishes a fundamental-rights framework within which statutory powers must operate. The experience of public-health governance illustrates this relationship. During the COVID-19 pandemic, governmental use of personal and health information generated substantial questions concerning the relationship between public necessity and individual privacy (Dar & Wani, 2022). A public emergency may justify broader data processing in appropriate circumstances, but emergency objectives do not automatically eliminate constitutional safeguards. The principal danger associated with the datafied State may not be the collection of individual pieces of information but their aggregation. A person's address, financial information, employment records, travel history and communications may reveal limited information. When combined, however, they can produce an extensive picture of individual behaviour.

This creates an important distinction between data points and data profiles. The privacy implications of a profile may be considerably greater than those of the individual pieces of information from which it is constructed. The problem also extends to information that is technically transformed or pseudonymized. Research concerning privacy-preserving textual representations demonstrates that technological transformations do not necessarily eliminate all privacy risks (Kim, Kim & Cho, 2026). The same concern is visible in discussions concerning genomic information, where technological advances have increased both the usefulness and sensitivity of personal biological information (Erdmann, 2013). The State's ability to generate inferences from existing databases therefore requires constitutional scrutiny even where no additional information has been directly collected.

Privacy must also be balanced against legitimate demands for governmental transparency. The existence of a public-interest justification for disclosure, however, does not mean that all government-held personal information should become publicly accessible. In *Hari C.V. v. Indian Institute of Information Technology* [2025 SCC OnLine Ker 4370], court recognised privacy considerations concerning personal and professional information in access under the RTI framework. The distinction is important because the datafied State creates two potentially competing risks, excessive secrecy and excessive disclosure. Government transparency may require access to information concerning public administration, but unnecessary disclosure of personal information may violate individual privacy. The broader literature similarly demonstrates the tension between personal-data protection and public-access interests (Brewczyńska, 2022). The appropriate approach is therefore to examine the purpose and public significance of the requested information rather than treating either privacy or transparency as an absolute principle.

Constitutional privacy cannot depend entirely upon judicial intervention after information has already been accessed. Effective protection requires safeguards operating throughout the data lifecycle. These safeguards should include clearly defined access permissions, purpose-specific processing, retention limits, security controls, audit mechanisms and independent oversight. The importance of institutional safeguards is recognised within broader international data-protection scholarship (Lokesh, 2021). Comparative analysis of Indian and European data-protection frameworks also illustrates the significance of principles such as purpose limitation, accountability and structured restrictions on processing (Narayan & Aggarwal, 2023). Government agencies should consequently maintain records of who accessed information, the purpose of access and extent of information retrieved. Where access involves particularly sensitive information, stronger safeguards should apply. Meaningful remedies are equally important. An individual should be able to challenge unlawful access and obtain appropriate relief where governmental processing violates constitutional or statutory requirements.

CONTEMPORARY JUDICIAL DIRECTION

The judiciary continue to recognize privacy as relevant to technologically mediated surveillance and information access. In *Prasath C. v State of Kerala* [2025 SCC OnLine Ker 1120], court considered the constitutional requirements governing State interference with privacy and reiterated the importance of legality, legitimate State objectives and proportionality.

In *Mr. Shuvendra Mullick v. Mr. Indranil Mullick* [2025 SCC OnLine Cal 2848], court addressed technological surveillance and held that continuous recording affecting private residential space could implicate the right to privacy. Although these cases do not establish a comprehensive constitutional code for executive data access, they reflect a broader judicial recognition that technological methods of observation and information processing can generate serious privacy concerns. The emerging jurisprudence therefore supports an approach in which the intensity of privacy interference is assessed rather than merely asking whether information is technically accessible.

India's future privacy framework should regulate the complete lifecycle of personal information rather than concentrating exclusively on initial collection. Six principles are particularly significant. First, legality requires a clear statutory foundation for governmental access. Second, purpose limitation requires information to be used for defined and legitimate objectives. Third, necessity requires the government to demonstrate why particular information is required. Fourth, proportionality requires consideration of less intrusive alternatives. Fifth, accountability requires institutional safeguards, auditing and oversight. Sixth, remedies require individuals to have meaningful mechanisms for challenging unlawful access.

These principles are consistent with the broader development of data-protection law internationally. Comparative scholarship demonstrates that jurisdictions have adopted different regulatory approaches, but protection against excessive governmental or institutional access remains an important component of contemporary privacy law (Muhammad, 2023). The social dimension of privacy must also be considered. Public attitudes towards privacy and data protection influence the legitimacy of governmental data practices (Sarabdeen & Moonesar, 2018). The evolution from early technological discussions of personal-data privacy to contemporary data-protection regimes demonstrates the scale of this transformation (Bogumil, 1983). Privacy is no longer concerned simply with whether information is physically observed. It concerns the capacity to collect, connect, infer and act upon information.

Conclusion And A Way Forward

The datafied State has fundamentally altered the relationship between governmental power and individual privacy. The State's ability to collect and process personal information can improve governance, but it simultaneously creates the possibility of unprecedented informational surveillance and profiling. Indian constitutional law provides an important framework for addressing this challenge. Privacy under Art. 21 protects informational interests and requires State interference to satisfy constitutional standards of legality, legitimate purpose, necessity and proportionality. The central principle should be that government possession of personal information does not amount to unrestricted governmental ownership of that information. Information collected for one purpose should not automatically become available for every subsequent governmental purpose. Nor should technological capacity be confused with constitutional authority.

The DPDPA, 2023 provides an important statutory foundation, but constitutional privacy must continue to operate as an independent limitation on executive power. As data becomes increasingly central to governance, India requires a framework that regulates not only collection but also access, aggregation, inference, retention and sharing. The future of informational privacy will therefore depend upon whether technological governance remains subject to constitutional limits. A democratic State may legitimately use personal data to perform public functions, but that power must remain bound by legality, necessity, proportionality, accountability and meaningful remedies.

References

1. Canayaz, M., Kantorovitch, I., & Mihet, R. (2021). Privacy laws and value of personal data. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3986562>
2. Agarwal, V. (2012). Privacy and data protection laws in India. *International Journal of Liability and Scientific Enquiry*, 5(3/4), 205. <https://doi.org/10.1504/IJLSE.2012.051949>
3. Sahoo, D. R. (2026). The data privacy laws in India: A legal analysis of Digital Personal Data Protection Act-2023. *International Journal of Latest Technology in Engineering, Management & Applied Science*, 15(7), 486–496. <https://doi.org/10.51583/IJLTEMAS.2026.150700040>
4. Kumar, H., Saraf, R., & Singh, S. (2024). Recent developments in data privacy laws in India. *PinG Privacy in Germany*, (2). <https://doi.org/10.37307/j.2196-9817.2024.02.07>
5. Singh, S., Inuganti, S., & Sahay, A. (2026). Recent developments in data privacy laws in India. *PinG Privacy in Germany*, (5). <https://doi.org/10.37307/j.2196-9817.2026.05.09>
6. Saha, S., & Mukhopadhyay, S. (2024). A new age of data privacy laws in India: Review of Digital Personal Data Protection Act, 2023. *International Journal of Law and Social Sciences*, 10(1), 84–95. <https://doi.org/10.60143/ijls.v10.i1.2024.114>
7. Wadman, M. (1997). US privacy laws may curb access to medical data. *Nature*, 386(6625), 533. <https://doi.org/10.1038/386533a0>
8. Park, H., Oh, H., & Choi, J. K. (2023). A consent-based privacy-compliant personal data-sharing system. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3311823>
9. Dar, M. A., & Wani, S. A. (2022). COVID-19, personal data protection and privacy in India. *Asian Bioethics Review*. <https://doi.org/10.1007/s41649-022-00227-0>
10. Huang, T., & Zheng, S. (2023). Using differential privacy to define personal, anonymous and pseudonymous data. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3321578>
11. Singh, A., & Chauhan, P. S. (2024). Transformative privacy: Analyzing the development of privacy rights and data protection laws in India. *International Journal of Multidisciplinary Trends*, 6(8), 55–59. <https://doi.org/10.22271/multi.2024.v6.i8a.468>

12. Kim, J., Kim, Y., & Cho, S. (2026). Personal embedding transformation for privacy-preserving split learning on textual data. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2026.3668872>
13. Erdmann, J. (2013). As personal genomes join big data will privacy and access shrink? *Chemistry & Biology*, 20(1), 1–2. <https://doi.org/10.1016/j.chembiol.2013.01.008>
14. Patel, A. (2025). Data protection and privacy laws. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5159813>
15. López, F. (2020). Privacy of personal data. *Revista Tecnologías de la Información y Comunicaciones*. <https://doi.org/10.35429/JITC.2020.11.4.8.11>
16. Lokesh, S. (2021). Privacy laws and regulations for safeguarding personal information in global data protection frameworks. *Law and Social Science Periodical*, 1(1). <https://doi.org/10.56106/lss.2021.004>
17. Narayan, A., & Aggarwal, P. (2023). Data protection and privacy laws currently in India with contrast to Europe. *International Journal of Scientific Research in Engineering and Management*, 7(3). <https://doi.org/10.55041/IJSREM18286>
18. Brewczyńska, M. (2022). Privacy and data protection vs public access to entrepreneurs' personal data. *European Law Blog*. <https://doi.org/10.21428/9885764c.4129f4be>
19. Hwang, T.-H., Shi, J., & Lee, K. (2023). Enhancing privacy-preserving personal identification through federated learning with multimodal vital signs data. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3328641>
20. Muhammad, Y. (2023). Data privacy laws in the USA. *International Journal of Information Privacy, Security and Integrity*, 5(3), 238–249. <https://doi.org/10.1504/IJPSI.2023.131571>
21. Sarabdeen, J., & Moonesar, I. A. (2018). Privacy protection laws and public perception of data privacy. *Benchmarking: An International Journal*, 25(6), 1883–1902. <https://doi.org/10.1108/BIJ-06-2017-0133>
22. Schwartz, P. M. (2004). Property, privacy, and personal data. *Harvard Law Review*, 117(7), 2056–2128. <https://doi.org/10.2307/4093335>
23. Bogumil, R. J. (1983). Technology and personal data privacy. *IEEE Technology and Society Magazine*, 2(2), 2–26. <https://doi.org/10.1109/MTAS.1983.5009771>
24. Berisha, I. S., Kerka, E. P., & Andersons, A. (2026). Personal data protection and privacy. *European Journal of Economics, Law and Social Sciences*, 10(1), 84–94. <https://doi.org/10.2478/ejels-2026-0009>
25. Muhammed, F., & Kachari, S. (2025). Surveillance, privacy and the policy challenges: Decolonizing personal data protection in India. *Journal of Digital Media & Policy*. https://doi.org/10.1386/jdmp_00177_1
26. Gandhi, M., & Gupta, A. (2020). A compendious analysis: Privacy protection laws in India. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3694664>
27. Shahnaz, S. K. (2024). Personal laws and women rights in India. *International Journal of Science and Research*, 13(2), 794–797. <https://doi.org/10.21275/MR24205093039>
28. Guidelines for recordkeeping under privacy and open-access laws. (1980). *Social Work*. <https://doi.org/10.1093/sw/25.6.452>
29. Nyoni, P., & Velepini, M. (2015). Data protection laws and privacy on Facebook. *SA Journal of Information Management*, 17(1). <https://doi.org/10.4102/sajim.v17i1.636>