Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Recalibrating Informational Privacy: A Constitutional Critique of India's Digital Personal Data Protection Act 2023

Ananya P[a]

[a]Ramaiah College of Law, Bengaluru, India

Received 01 April 2026; *Accepted* 05 May 2026; *Published* 09 May 2026

The passing of the Digital Personal Data Protection Act 2023[1] *(DPDP Act) is the first time that India has tried to regulate personal data in the digital era. The Act was born out of the landmark case of Justice K.S. Puttaswamy v Union of India*[2]*, where the Supreme Court of India held that the right to privacy is a fundamental right guaranteed by the Constitution of India. This paper, however, suggests that the DPDP Act diverges from the rights-based approach and adopts a State-centric approach to governing data. Based on both doctrinal and comparative analysis, this paper analyses the features of the DPDP Act, such as consent, State exemptions, institutional designs, and individual rights, to suggest that the DPDP Act fails to meet the constitutional standards, especially those of proportionality laid down under Article 21 of the Constitution. Comparing the DPDP Act to the GDPR and other laws globally, this paper identifies significant lacunae in India's data protection legislation. It recommends a move towards digital constitutionalism in this regard.*

Keywords: *data protection, privacy, informational privacy, constitutional law, surveillance*

1 Digital Personal Data Protection Act 2023

2 *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

INTRODUCTION

The fast development of digital technology has made data a key component in governance, economic prosperity, and social organisation. Digital infrastructures like e-governance portals and digital identification systems have resulted in the collection of a lot of personal data by state and private bodies in India. India did not have an adequate law regulating data protection until recently, when *Justice K.S. Puttaswamy v Union of India (2017)* was decided. The case led to the recognition of the right to privacy as a fundamental right guaranteed by Article 21 of the Constitution, as it is intrinsic to dignity, autonomy, and freedom. Informational privacy is recognised as a necessity, which requires an appropriate regulatory system. Thus, the Digital Personal Data Protection Act 2023 has been developed as a response. Despite being a positive step in protecting personal information, the legislation raises issues concerning its adequacy and constitutionality. Therefore, this paper aims to analyse whether the Act achieves an effective balance between the competing interests or gives preference to the State and economic interests over individual rights. It is argued that the DPDP Act is a failure in balancing state powers and individual rights because it reflects governance priorities rather than a rights-based approach.

METHODOLOGY

This study adopts a doctrinal and analytical approach to evaluate the DPDP Act within the framework of Indian constitutional law and comparative data protection regimes. It relies on statutory interpretation and judicial precedents concerning privacy, autonomy, and State power.

A comparative analysis with frameworks such as the EU's General Data Protection Regulation (GDPR) is undertaken to assess the Act against globally accepted principles of transparency, accountability, and individual rights. Primary sources include legislation, judicial decisions, and committee reports, while secondary sources include scholarly literature and policy analyses. The analysis is grounded in the doctrine of proportionality, as articulated in *Puttaswamy*, alongside the concept of informational self-determination, which emphasises individual control over personal data.

EVOLUTION OF DATA PROTECTION LAW IN INDIA

Fragmented Pre-Legislative Data Protection Framework: Before the enactment of the Digital Personal Data Protection Act 2023, the Indian legislative landscape for data protection law was characterised by fragmentation and inefficacy. This can be attributed to the reliance on the Information Technology Act 2000 and the SPDI Rules of 2011. In terms of the nature of applicability, however, it is imperative to note that these laws did not apply to all types of personal information but rather focused on sensitive personal data. As such, there existed substantial lacunae in their coverage and application. Moreover, compliance requirements stipulated under these statutes were few and ineffective, thus failing to achieve adequate regulation of data handlers. The lack of effective enforcement and institutional capacity made matters worse by undermining the legal standing of individuals in the event of data infringement.

Privacy as a Fundamental Right under the Indian Constitution: One of the important landmarks in the journey of data protection laws in India was the judgment delivered by the Hon'ble Supreme Court of India in the case of *Justice K.S. Puttaswamy v Union of India.*[3] In the above-stated case, it was held by the Supreme Court, through a unanimous judgment, that the right to privacy constitutes an integral part of Article 21 of the Indian Constitution, read along with Article 14 and Article 19. The said case established the fact that privacy forms an indispensable part of life, liberty, and dignity. Furthermore, the judgment established the concept of informational privacy as an integral component of the right to privacy, which necessitates the regulation of information and its collection from individuals. In addition to the above, the Court laid down an elaborate proportionality test which mandates that any form of restriction imposed upon the right to privacy shall have to be legal, having a legitimate aim, necessary, and proportional.

Developments in Legislation: Following the guidelines set out by Puttaswamy, the Government of India appointed a committee under Justice B.N. Srikrishna, known as the Justice B.N. Srikrishna Committee, in 2017 [4]to investigate the concerns surrounding data protection legislation. According to the report by the Committee submitted in 2018, it was argued that a proper data protection system should be based on fundamental rights,

[3] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1
[4] B N Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

including data minimisation, limitations on purpose, and accountability. Moreover, the notion of 'data fiduciaries' came up within the report, highlighting the disparity of power between the individual and the organisation processing their personal data. It was later observed that there had been a divergence from the earlier stance taken by the legislation. As evident from the changes made in successive drafts of the data protection bill, there has been a trend toward increased powers of the State while reducing individual protections at the same time. With a focus on greater governance efficiency and economic considerations, the Digital Personal Data Protection Act, 2023, came into existence.

LITERATURE REVIEW

The debate surrounding issues such as data protection and information privacy in India has come a long way over the last few years, especially with the constitutionalisation of privacy as a basic right. Much of the research conducted has dealt with the ethical foundations of privacy, the structure of data protection law, and the dynamics of power between the State and the individual.

In early literature post the *Justice K.S. Puttaswamy v Union of India* case, privacy was identified as an important aspect of dignity and freedom. According to Gautam Bhatia[5], privacy should be seen as an institution that protects both State and non-state actors. Apar Gupta, on the other hand, points out the growing danger posed by digital surveillance systems and the importance of having stringent procedural safeguards in any data protection law.

The Justice B.N. Srikrishna Committee Report (2018) is a seminal contribution to data protection literature in India. The committee recommended an extensive structure based on the guiding principles of data minimisation, purpose limitation, and accountability. One significant contribution of the committee was the idea of 'data fiduciaries', which acknowledged the imbalance of power relations when it comes to individual data processors. Nevertheless, recent studies have suggested that the DPDP Act[6] largely diverges from the committee's suggestions, especially regarding state exemptions and regulatory independence.

[5] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins 2019)
[6] Digital Personal Data Protection Act 2023

The literature on data protection in India has been enriched by comparative research focusing on EU legislation. For instance, Paul De Hert and Vagelis Papakonstantinou[7] highlight the importance of rights-based approaches to data protection embodied in the General Data Protection Regulation (GDPR). As opposed to this, some Indian researchers suggest that the DPDP Act has a state-centred approach.

Consent as a mechanism of regulation is also being questioned in contemporary literature. Authors like Solove have argued against the 'privacy self-management' theory[8], claiming that people cannot exercise their consent because of the information imbalance and cognitive dissonance. This issue is very pertinent for India, where there is no uniformity in the level of digital literacy.

A new academic paradigm in this field has emerged that discusses the theory of 'digital constitutionalism,' which aims to incorporate constitutional principles into the digital age. The theory is extremely important in analysing the DPDP Act since it stresses that both state and private entities must be subjected to constitutional principles, especially regarding fundamental rights.

In conclusion, modern literature is rife with the existence of two competing theories in privacy regulations: one is based on rights that focuses on personal freedom, while the other is focused on governance and flexibility of the state and economy. The DPDP Act will be analysed in this context.

CONCEPTUAL FOUNDATIONS

Informational Privacy and Autonomy: While information privacy entails the defence of secrets, it encompasses much more than that; it involves individuals' capacity to control the flow and use of their personal information. Such capacity is fundamental to exercising the right to autonomy, self-respect, and free speech. Otherwise, individuals become susceptible to profiling, monitoring, and behavioural manipulation; democracy itself becomes

[7] Paul De Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32(2) Computer Law & Security Review 179 <https://sciencedirect.com/science/article/abs/pii/S0267364916300346> accessed 29 March 2026

[8] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880 <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2093&context=faculty_publications> accessed 29 March 2026

impossible. Hence, information privacy should not be regarded as a standalone legal issue but as a cornerstone of constitutional democracy.

Data as Power: Moreover, the governance of personal data should not only be viewed from the perspective of regulation but also from the perspective of power. In today's digital environment, data constitutes a vital source of economic and political power. Consequently, there have been notable disparities between individuals on one hand and companies or State institutions on the other. On the one hand, individuals or data subjects/data principals lack the knowledge and means to govern the process of data processing. On the other hand, companies and State institutions have the technological means to gather and analyse huge amounts of data for economic or political purposes. Therefore, there is a need for regulatory measures to address such inequalities.

Consent and Its Limitations: Historically, consent has been considered the foundation of privacy legislation because it is based on the principle that individuals should be in charge of determining what is done with their personal data. Unfortunately, in reality, there are multiple reasons why the efficacy of the process of providing consent has proven to be seriously flawed. To begin with, privacy policies are usually complicated and hard to understand, which makes it virtually impossible to provide any kind of informed consent. Next, the dominance of 'take it or leave it' models within online platforms implies that users can only give consent under pressure. Lastly, often the unavailability of any other options makes consent useless.

KEY FEATURES OF THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Consent-Based Model: The Digital Personal Data Protection Act 2023[9] follows a consent-based model in the processing of personal data. According to the Act, this consent should be voluntary, specific, informed, and unequivocal, thus meeting the globally accepted standards. Such a model is designed to protect the interests of individuals by processing data solely based on their consent. However, the notion of 'deemed consent' greatly undermines the very foundation of such a consent-based model. By allowing data processing without consent under certain conditions, the Act disregards individual rights and control over their data.

[9] Digital Personal Data Protection Act 2023

Rights of Data Principles: Several rights are granted to individuals who can be called data principals through the Act, with the intention of improving the level of accountability. The rights include the right to get access to information on how one's data is being processed, the right to correction of one's data, the right to erasure of data that is unnecessary or inaccurate, and finally the right to resolve grievances. Although such rights are significant in the recognition of personal interests, their efficacy depends on effective mechanisms of implementation.

Duties of Data Fiduciaries: In terms of duties of data fiduciaries, the Act imposes a number of them. In general, these duties refer to the duty to ensure proper security of the processed data, notification procedures in case of data breaches, and compliance with the principle of purpose limitation, according to which any data should be processed only for certain legitimate purposes. Furthermore, those organisations, which are referred to as Significant Data Fiduciaries, have even higher duties due to increased risks related to large-scale processing of data. Nevertheless, such efforts to strengthen accountability can hardly produce the desired effect without strict enforcement.

Data Protection Board: Under the Digital Personal Data Protection Act 2023, the Data Protection Board acts as the main regulatory body accountable for enforcement and adjudication. It has been entrusted with the responsibility of redressal of grievances, compliance with the law, and punishing violators. However, there exist certain problems with respect to its independence, considering that its members are nominated by the Central Government itself. In this context, issues related to objectivity and impartiality come up when dealing with matters of State institutions.

CRITICAL ANALYSIS

Wide State Exemptions: Perhaps one of the most controversial elements of the DPDP Act is the wide range of exemptions accorded to the State. It allows the Central Government to exempt its departments for reasons including national sovereignty, security of the State, and public order. Though these are valid concerns, the lack of specific safeguards creates significant constitutional issues.

As per *People's Union for Civil Liberties vs Union of India*[10], telephone tapping amounts to a violation of privacy rights except when it follows the procedure established by law. Among the safeguards put in place are prior authorisation, time limits, and review. They were implemented to ensure that there was no arbitrary invasion of privacy. However, the DPDP Act lacks similar safeguards, which may lead to abuse of executive power.

Dilution of Consent: 'Deemed Consent' marks a huge erosion in the importance of consent as a tool to protect informational privacy. As the DPDP Act provides for several situations where processing personal information does not require consent, it deviates from the concept of informed consent. It becomes especially troubling in view of the judgment in *K.S. Puttaswamy (Aadhaar) v Union of India*[11], where, while endorsing the Aadhaar regime, the Court imposed various restrictions on the system, which included data minimisation, purpose limitation, and proportionality, taking into consideration dangers like exclusion and exploitation. It clearly states that efficiency cannot trump constitutional values. The use of deemed consent in the DPDP Act contravenes this value.

Poor Institutional Structure: The institutional structure of the Data Protection Board appears to be problematic in terms of its independence and accountability. In view of the fact that members of the Board are selected by the Central Government, the institution is not structurally autonomous to act with objectivity in the decision-making process. This becomes even more important given the recent judgment of the Supreme Court in the case of *Anuradha Bhasin v Union of India*[12], wherein it was highlighted that any limitation upon fundamental rights must be rational, proportionate, temporary and subject to review. Transparency in terms of publishing orders is an important element that must be considered.

Individual Rights Restricted: Further, the restrictions on individual rights contained in the Act weaken its efficiency even more. Although it grants the basic rights of access and correction, it lacks essential rights, including data portability and an overarching right to be forgotten. The Indian judiciary has recognised these rights in diverse situations, signalling a rising awareness of information self-determination. This lack of these rights in legislation

[10] *People's Union for Civil Liberties v Union of India and Anr* (1997) 1 SCC 301
[11] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2019) 1 SCC 1
[12] *Anuradha Bhasin v Union of India* AIR 2020 SC 1308

signals a separation between judicial progress and legislative intent, thus hampering the empowerment of data principals.

Surveillance Issues: The combined impact of wide-ranging State exemptions, weakened consent, and insufficient institutional controls could result in an environment conducive to pervasive surveillance. This would have serious consequences for the democratic liberties of the citizens. As noted in *Anuradha Bhasin v Union of India*, restrictions on internet access have a 'chilling effect' on the right to freedom of speech and expression. Likewise, a data protection regime that permits widespread surveillance without sufficient protections is likely to discourage the exercise of fundamental rights.

Justifications for a Flexible State-oriented Model: It should also be noted that there is some legitimacy in the approach adopted by the State in light of the DPDP Act[13]. In light of a developing digital economy like that of India, the need for flexible regulation to foster innovation, enhance efficiency, and safeguard national security cannot be overlooked. It can be argued that the State requires greater flexibility in its regulation than that offered by rights-centric models like the GDPR in a country that lacks uniformity in its level of digital literacy.

Governance structures such as welfare systems and digital identification mechanisms involve large volumes of data processing, which makes a flexible approach to the use of data a practical consideration. Nonetheless, this flexibility cannot supersede constitutional constraints. In Puttaswamy (Aadhaar), it was made clear that considerations of efficiency cannot take precedence over basic constitutional rights. Even where the State has valid interests, the principles of legality, necessity, and proportionality must be fulfilled.

COMPARATIVE ANALYSIS

European Union (GDPR): The General Data Protection Regulation (GDPR) of the European Union[14] has been viewed as an exemplar for data privacy laws. The regulation embraces the idea of protecting individual rights by emphasising individual agency and responsibility. Under the GDPR, strict criteria have to be met for consent acquisition; data must be processed transparently; and there are several important rights for individuals, such as the right to data

[13] Digital Personal Data Protection Act 2023
[14] General Data Protection Regulation (GDPR) 2016

portability and the right to be forgotten. What's more, it creates independent supervisory bodies responsible for ensuring its enforcement.

India's Divergence: However, there is a notable difference between India's DPDP Act, 2023[15] and GDPR[16], as the former is much more flexible and State-oriented in its approach. Although the Act acknowledges the relevance of giving consent, the introduction of 'deemed consent' renders it considerably less efficient compared to the GDPR. In other words, while GDPR makes explicit consent an essential component of data protection measures, the Indian law does not pay much attention to it.

Another important difference between the two acts relates to the rights granted to individuals. For example, the DPDP Act gives individuals a more modest set of rights as it fails to address such important provisions of data protection as data portability. Moreover, the independent bodies mentioned in the Act cannot be viewed as analogues of the GDPR supervisory authorities. Last but not least, one of the most fundamental differences between the GDPR and the DPDP Act is related to the position the former takes concerning state authorities' access to personal data. Unlike GDPR, the Act in question offers numerous exceptions for government entities regarding data access requirements.

United States and United Kingdom: The examples of data protection models used in the USA and UK demonstrate additional diversification in the field. For the most part, the USA implements a sectoral approach to protecting personal information based on multiple laws dedicated to specific areas (health and finance). Although this method makes it possible to regulate industries effectively, it is considerably less coherent and consistent than comprehensive frameworks like the GDPR.

On the other hand, the UK continues to pursue the GDPR principles through its data protection framework even after its Brexit from the European Union. In particular, the UK places a substantial emphasis on individual rights, transparency, and the autonomy of the regulator. Moreover, the UK Information Commissioner's Office serves as an autonomous regulatory body responsible for both public and private spheres. Therefore, India's DPDP Act can be regarded as a mixture of two approaches, which fail to reach their best qualities

[15] Digital Personal Data Protection Act 2023
[16] General Data Protection Regulation (GDPR) 2016

due to its hybrid nature. Namely, it cannot provide the same level of rights protection as the GDPR or achieve a similar degree of specificity found in the US framework.

RECONCEPTUALISING DATA PROTECTION IN INDIA: AN ORIGINAL CONTRIBUTION

The Digital Personal Data Protection Act 2023[17] should not be viewed solely as a law regulating data processes but as the basis for the new relationship between the citizen, the State, and private entities in the digital era. The central thesis of this paper is that the DPDP Act introduces a move away from rights-oriented models of data protection toward administrative governance models of data regulation. The key characteristics of such a model would include an understanding of data protection not as an extension of the right but rather as a form of regulation emphasising efficiency and flexibility.

This reconceptualisation carries substantial legal implications for data protection law. It goes against the judicial doctrine developed in the landmark case of *Justice K.S. Puttaswamy v Union of India*[18], according to which informational privacy can be treated as an inherent part of human dignity and liberty and thus requires the implementation of a rights-centric approach to regulating the field. Yet the DPDP Act undermines such a paradigm by introducing wide-ranging State exemptions, weak consent requirements, and limited individual rights.

In view of this paradigm shift, it becomes imperative to re-evaluate the foundations upon which the data protection regime in India must be grounded. One such way could be the adoption of digital constitutionalism, through which constitutional guarantees are extended to the digital world. The constitutional implications of the data protection law would then mean that both state and non-state entities that engage in the processing of personal information would be required to meet constitutional standards, especially in respect of Articles 14, 19, and 21.

It is further proposed that judicial oversight procedures be incorporated in the Act for granting exemptions by the State. Taking cues from the constitutional jurisprudence on surveillance powers and executive powers, State exemptions based on considerations such as national security and public order would require prior authorisation or review by courts.

[17] Digital Personal Data Protection Act 2023
[18] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

Such a measure would bring the Act in line with the emphasis on procedural safeguards in *People's Union for Civil Liberties v Union of India*[19].

Moreover, the regulatory scheme must not be limited merely to consent alone and must embrace substantive duties based on principles of equity and accountability. Indeed, as noted in *K.S. Puttaswamy (Aadhaar) v Union of India*[20], principles like data minimisation and purpose limitation play a crucial role in providing adequate safeguards for protecting privacy rights. Inclusion of these principles in the statutory scheme will contribute to the further improvement of individuals' rights.

At the end of the day, the successful operation of any regime of data protection must strike an appropriate balance between the demands of technology and the constitutional ideals. The current DPDP Act embodies this inequality between them and emphasises governance efficiency. This problem must be solved by recalibrating the regulatory scheme through digital constitutionalism and institutional independence.

CONSTITUTIONAL ANALYSIS

The DPDP Act must be assessed based on the principles of proportionality as laid out in *K.S. Puttaswamy v Union of India*. Though the DPDP Act complies with the formal aspect of legality, the substantive part fails in terms of necessity and proportionality.

The wide exceptions that have been made in favour of the State lack precision, and the lack of procedural safeguards fails to justify the State's interest vis-à-vis an individual's right. In the case of *K.S. Puttaswamy (Aadhaar) v Union of India*, it is evident that there must be strong safeguards for data-based governance, and the case of *People's Union for Civil Liberties v Union of India* shows the significance of procedural safeguards in surveillance. Thus, it can be said that the DPDP Act fails in terms of the constitutional test.

CONCLUSION

With the advent of the Digital Personal Data Protection Act 2023, India is at an inflexion point in the legal development of data protection laws. It may be seen as the first step by the State to regulate the protection of personal data in the digital space. Nevertheless, while being

[19] *People's Union for Civil Liberties v Union of India and Anr* (1997) 1 SCC 301
[20] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2019) 1 SCC 1

progressive legislation, it still fails to create a strong, rights-oriented framework to protect informational privacy.

While reading Justice K.S. Puttaswamy v Union of India and *Anuradha Bhasin v Union of India*[21], one can understand that the State must make efforts to protect individual autonomy from being excessively interfered with. In turn, the DPDP Act introduces a different vision, which gives precedence to the administrative flexibility of government over constitutional obligations.

Given this, in order to achieve coherence with domestic and international laws, the DPDP Act requires a revision to introduce stronger restrictions on the State's authority, better enforcement mechanisms, and greater emphasis on individual rights. In particular, this means including proportionality rules, limiting the State's exceptions, granting greater independence to authorities, and increasing individual rights available to data principals.

More generally, the constitutional dilemma presented by the DPDP Act reflects a much larger question about regulating digital power in such a way that democracy is safeguarded. Informational privacy can no longer be considered an ancillary matter but rather an integral part of the constitutional framework. Any further development of data protection legislation in India needs to transcend mere compliance to include substantive protection in such a way that innovation does not come at the expense of fundamental human values.

In any event, the validity of the regulatory framework governing India's digital world cannot be established through efficiency alone but rather requires constitutional fidelity. In order to create a paradigm-shifting data protection scheme, it is essential to keep the individual at the forefront, as only then can it be truly said that the most sophisticated exercise of State power is still bound by the Rule of Law.

[21] *Anuradha Bhasin v Union of India* AIR 2020 SC 1308