The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

BALANCING PRIVACY AND POWER: A CRITICAL STUDY OF INDIA'S DATA PROTECTION REGIME AFTER PUTTASWAMY

~ Harshita Rana

ABSTRACT

The digital revolution has fundamentally altered the interaction between the individual, the state, and the market, necessitating a re-evaluation of the legal principles governing personal information. In India, this evolution was anchored by the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[1], which unanimously recognized the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21. This research paper explores the trajectory of India's data protection regime, tracing its origins from early restrictive precedents to the contemporary statutory framework. It critically analyzes the *Digital Personal Data Protection (DPDP) Act, 2023*, evaluating its ability to operationalize the constitutional principles of informational privacy, autonomy, and dignity and drawing the comparison with EU's general data protection regulation. By examining the robust proportionality test established in Puttaswamy and its application in subsequent cases like the Aadhaar judgment and the *Pegasus controversy*, the study highlights a growing tension between individual rights and state power. The research identifies significant structural concerns, including the broad exemptions granted to government agencies under Section 17 and the perceived lack of institutional independence for the Data Protection Board of India. The paper concludes that while the DPDP Act is a milestone, its effectiveness in safeguarding privacy against corporate and state overreach depends on narrow judicial interpretation of exemptions and the strengthening of regulatory oversight to prevent the "new oil" of data from becoming a tool of unchecked surveillance.

[1] *(2017) 10 S.C.C. 1.*

Keywords: Right to Privacy, Puttaswamy Judgment, Digital Personal Data Protection Act (DPDP), Informational Privacy, Proportionality Test, Data Fiduciary, State Exemptions.

1. Introduction

In the contemporary global landscape, data has emerged as the most critical resource, often described as the "lifeblood" sustaining political, social, and commercial decisions. The expansion of digital communication, e-governance, and artificial intelligence has created a environment where personal information is continuously generated, aggregated, and processed. While this data-driven economy offers immense potential for innovation and efficiency, it simultaneously creates profound risks to individual autonomy and human dignity. Data breaches, algorithmic profiling, and unauthorized surveillance have intensified concerns regarding privacy in democratic societies.

Historically, India lacked a comprehensive, standalone legislation to address these challenges. Privacy protections were fragmented across the Information Technology Act of 2000, various sectoral regulations, and incremental judicial decisions. This legal vacuum was conclusive addressed by the judiciary. The recognition of privacy as a fundamental right in the Puttaswamy ruling marked a paradigm shift, providing the normative foundation for a rights-based data protection regime.

The journey toward a comprehensive data protection regime in India has been a long-drawn legal evolution, transitioning from an era of judicial hesitation to a constitutionally mandated framework centered on human dignity.

The History and Evolution of Privacy in India

For the first few decades of the Republic, the Indian judiciary adopted a restrictive and fragmented view of personal rights. This "isolated silos" approach, often called the Gopalan doctrine, viewed fundamental rights as mutually exclusive rather than interconnected.

In the 1954 case of *M.P. Sharma v. Satish Chandra*[2], an eight-judge bench ruled that the Constitution did not explicitly protect a right to privacy in the context of state search and seizure operations. This was followed by the 1962 *Kharak Singh v. State of Uttar Pradesh*[3] ruling, where a six-judge bench examined police surveillance involving "midnight knocks". While the majority struck down nocturnal visits as a violation of personal liberty, they explicitly stated

[2] *(1954) 1 S.C.R. 1077*
[3] (1964) 1 S.C.R. 332

that a fundamental right to privacy did not exist under the Constitution. A critical turning point was the dissent of Justice Subba Rao in Kharak Singh, who argued that "personal liberty" was a comprehensive term including the right to be free from encroachments on one's private life. He famously noted that psychological restraints and constant surveillance could be as damaging to human happiness as physical imprisonment.

Following the shift toward a more cohesive reading of rights in the 1970s, the judiciary began to infer privacy from existing guarantees. In *Gobind v. State of Madhya Pradesh*[4], the Court acknowledged a "penumbral" right to privacy, though it cautioned that this right was not absolute. Subsequent cases expanded this further, *R. Rajagopal v. State of Tamil Nadu*[5] recognized the "right to be let alone" against unauthorized publications, and the *PUCL* judgment extended privacy protections to telephone conversations.

The constitutional landscape was permanently transformed in August 2017 with the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[6]. Arising from a challenge to the Aadhaar biometric scheme, a nine-judge bench unanimously declared that privacy is an inherent fundamental right under Article 21 of the Constitution.

The Court conceptualized privacy as essential for autonomy, dignity, and self-determination. Justice Chandrachud identified three key dimensions: bodily privacy, decisional autonomy, and informational privacy. To ensure these rights weren't just a formality, the Court established a three-fold proportionality test for any state interference:

1. **Legality:** The action must be backed by a clear law.
2. **Legitimate Aim:** The state must have a valid reason (e.g., national security or welfare delivery).
3. **Rational connection and necessity:** There must be a rational nexus between the measures adopted and the objective sought to be achieved.
4. **Proportionality:** The benefit gained by the state must outweigh the harm caused to individual rights.

The Puttaswamy ruling created an immediate legislative mandate, the state was now obligated to develop a robust statutory framework to protect personal data. In response the government

[4] (1975) 2 S.C.C. 148
[5] (1994) 6 S.C.C. 632.
[6] *(2017) 10 S.C.C. 1.*

constituted The Srikrishna Committee shortly after the 2017 verdict, the Central Government constituted a Committee of Experts chaired by Justice B.N. Srikrishna. Their 2018 report, *"A Free and Fair Digital Economy,"* [7]became the blueprint for Indian data protection, proposing a rights-based framework centered on informed consent and institutional independence. Based on the committee's suggestions, the Personal Data Protection Bill, 2019 was introduced. However, it faced intense criticism for granting excessive exemptions to government agencies and was eventually withdrawn in August 2022 after a review by a Joint Parliamentary Committee. Thereafter the government introduced a simplified, more "business-friendly" version as the Digital Personal Data Protection Bill, 2023. It was passed by Parliament and received presidential assent on August 11, 2023, becoming India's first focused legislative attempt to regulate the digital data ecosystem. Today, the DPDP Act serves as the primary regulator for digital personal data, aiming to balance the individual's right to protect their information with the state's need to process data for lawful purposes and governance.

This study is particularly vital because it evaluates whether the DPDP Act effectively operationalizes the constitutional principles of proportionality and necessity established in Puttaswam*y*, or whether the broad exemptions granted to government agencies risk diluting the very rights the Act intended to protect.

To explore these complexities, this paper is structured to provide a comprehensive roadmap of the post-Puttaswamy landscape. It begins by tracing the evolution of privacy jurisprudence in India, moving from early restrictive precedents that denied a constitutional right to privacy to the eventual judicial recognition of its intrinsic link to human dignity. The analysis then shifts to a detailed examination of the Puttaswamy judgment, specifically focusing on the dimension of informational privacy and the four-pronged test used to evaluate state interference with individual rights.

The middle chapters provide a structural analysis of the DPDP Act, 2023, dissecting the rights of individuals such as access, correction, and erasure and the stringent obligations imposed on Data Fiduciaries. Central to this discussion is a critical evaluation of the balance of power, where the paper scrutinizes the contentious state exemptions under Section 17 and the institutional independence of the Data Protection Board of India. Finally, the study adopts a comparative perspective by drawing lessons from the EU's General Data Protection Regulation

[7] Justice B.N. Srikrishna committee, A *Free and fair digital economy: protecting privacy, empowering Indians (2018)*

(GDPR) and concludes with a set of suggestions aimed at harmonizing statutory provisions with the enduring spirit of the *Puttaswamy* vision.

II. The Evolution of Privacy Jurisprudence: Pre-Puttaswamy Precedents

Before the 2017 constitutional declaration, Indian privacy law developed through a series of often conflicting judicial interpretations that struggled to define the scope of Article 21.

.The Early Denial of Privacy

The history of the right to privacy in India is a story of gradual judicial awakening, moving from a period of strict literal interpretation of the Constitution to a deep recognition of privacy as an essential part of human dignity. In the early decades following independence, the legal landscape was dominated by the "Gopalan doctrine,[8]" which viewed fundamental rights as separate, watertight compartments rather than a unified web of protections. This restrictive view was clearly seen in the case of *M.P. Sharma v. Satish Chandra*[9], where an eight-judge bench addressed a challenge to a search and seizure operation. The Court held that the framers of the Constitution had not intended to create a fundamental right to privacy similar to the Fourth Amendment of the U.S. Constitution. At that time, the judiciary believed that in the absence of an express provision, privacy could not be read into other rights like the guarantee against self-incrimination.

This initial denial of privacy was further tested in the 1962 landmark case of *Kharak Singh v. State of Uttar Pradesh*[10]. The petitioner, who had been accused in a dacoity case but released for lack of evidence, was subjected to intrusive police surveillance, including "history-sheet" recording and "midnight knocks" or domiciliary visits at night. The majority opinion of the six-judge bench struck down the nightly visits as a violation of "ordered liberty" under Article 21, famously noting that "every man’s house is his castle". However, the majority simultaneously asserted that the right to privacy was not a guaranteed fundamental right, and they upheld other forms of surveillance like secret picketing. This created a logical inconsistency within the judgment protecting the sanctity of the home under Article 21 while denying the existence of a broader privacy right. A powerful dissent by Justice Subba Rao provided the intellectual spark for future change. He argued that "personal liberty" was a comprehensive term that included

[8] *1950 SCR 88.*
[9] *(1954) 1 S.C.R. 1077*
[10] *(1964) 1 S.C.R. 332*

the right to be free from encroachments on private life, suggesting that psychological restraints through surveillance could be just as damaging as physical imprisonment.

By the mid-1970s, the judiciary began to soften its stance, influenced by the shifting understanding that fundamental rights were overlapping and mutually reinforcing. In the 1975 case of *Gobind v. State of Madhya Pradesh*[11], the Supreme Court evaluated police regulations that allowed for the surveillance of "habitual criminals". While the Court ultimately dismissed the petition, Justice Mathew's judgment took a more nuanced approach by "assuming" for the sake of argument that an independent right to privacy could be an emanation from the existing guarantees of personal liberty and free movement. The Court suggested that if such a right existed, it would cover intimate matters like the home, family, and marriage, but it would not be absolute. Crucially, *Gobind* introduced the "compelling state interest" test, stating that any law infringing on a fundamental privacy right must be narrowly tailored to serve a superior state objective.

The evolution continued in the 1990s as the Court began to firmly root privacy within the right to life and liberty. In *R. Rajagopal v. State of Tamil Nadu* [12], often called the "Auto Shankar case," the Court dealt with the freedom of the press versus the privacy of a death row convict whose autobiography was being published. Justice Jeevan Reddy explicitly recognized that the right to privacy is implicit in Article 21 and described it as the "right to be let alone". The judgment clarified that individuals have a right to safeguard the privacy of their families, education, and health, and that unauthorized publications concerning these matters would constitute a violation unless they were based on public records. This decision was significant because it applied privacy principles to a dispute involving private parties and public officials, moving beyond the traditional context of police surveillance.

The 1996 case of *People's Union for Civil Liberties (PUCL) v. Union of India*[13] addressed privacy in the context of modern technology specifically, telephone tapping. The Court ruled that a telephone conversation is an intimate and confidential part of a person's life, and that intercepting it constitutes a serious invasion of privacy. Building on the foundations laid in Kharak Singh and Rajagopal, the Court held that Article 21 is attracted whenever the facts of a case constitute a right to privacy, and that such a right cannot be curtailed except through a "procedure established by law" that is just, fair, and reasonable. Because the government had

[11] (1975) 2 SCC 148
[12] (1994) 6 S.C.C. 632.
[13] (1997) 1 SCC 301.

not framed any rules to prevent the improper interception of messages, the Court felt compelled to lay down its own procedural safeguards to prevent arbitrary state action. Collectively, these cases demonstrate a persistent judicial journey toward recognizing privacy not as a vague abstract concept, but as a core constitutional value that protects the dignity and autonomy of every individual against both the "searching glare of publicity" and the overreach of the state.

The Seeds of Change: The Subba Rao Dissent

The dissent of Justice Subba Rao in Kharak Singh provided the early intellectual framework for Puttaswamy. He argued that "personal liberty" was a comprehensive term that included the right to be free from encroachments on private life. He famously noted that in an advancing civilization, psychological restraints and surveillance could be as deleterious to happiness as physical restraints.

III. The Constitutional Watershed: Analyzing Puttaswamy I

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[14] represents the definitive constitutional moment for privacy in India, resolving decades of judicial ambiguity and establishing the normative framework for the country's current data protection regime.

The Puttaswamy case originated from a 2012 challenge to the Aadhaar scheme, India's biometric-based national identity program. The petitioner, a retired High Court judge, argued that the government's mandatory collection of sensitive biometric and demographic data without a supporting legislative framework constituted a grave violation of the right to privacy. The Union Government contested this by citing early precedents, such as M.P. Sharma and Kharak Singh, which had suggested that privacy was not a fundamental right under the Indian Constitution. This direct conflict in jurisprudence led to the constitution of a nine-judge bench to authoritatively decide the status of privacy.

The Supreme Court unanimously declared that privacy is a constitutionally protected fundamental right. The Court moved away from the "Gopalan doctrine" of viewing rights in isolated silos, instead holding that privacy is an essential component of Article 21 (Right to Life and Personal Liberty) and is further enriched by the freedoms guaranteed under Article 14 (Equality) and Article 19 (Fundamental Freedoms). By doing so, the Court expressly overruled

[14] *(2017) 10 S.C.C. 1.*

the restrictive portions of the M.P. Sharma and Kharak Singh judgments that had denied privacy constitutional status.

The judgment identified informational privacy as a distinct and vital dimension of the right to privacy, particularly in a digital world. The Court recognized that in an age of data ubiquity, individuals have a right to control the dissemination and use of their personal data. It noted that "informational traces" left by digital activities are as personal as one's choice of appearance, and that the aggregation of such data can reveal intimate details of a person's life, thereby requiring stringent legal protection.

The Court conceptualized privacy as a "postulate of human dignity itself," asserting that it is essential for autonomy and self-determination. Privacy recognizes the "inner recesses of the human personality" and the right of every individual to make personal choices regarding their body, relationships, and reproductive health without unwarranted state interference. The "right to be let alone" was characterized as a manifestation of an inviolate personality, which allows the human being to be free from intrusions into their mental and physical being.

The Puttaswamy judgment established that personal data is not merely a commercial asset but is constitutionally connected to individual identity and personhood. Consequently, the Court imposed a positive obligation on the State to develop a comprehensive legislative framework to protect personal data. This constitutional mandate was the direct catalyst for the eventual enactment of the Digital Personal Data Protection (DPDP) Act, 2023, which was intended to operationalize the privacy principles established by the Court.

The Proportionality Test

To prevent the arbitrary exercise of state power, the Court articulated a rigorous four-pronged test (often referred to as the proportionality test) that any state interference with privacy must satisfy:

- **Legality:** The action must be sanctioned by a clear and valid law.
- **Legitimate State Aim:** The restriction must pursue a valid objective, such as national security, the prevention of crime, or the targeted delivery of welfare benefits.
- **Necessity:** The means adopted must be necessary for achieving the aim, and there must be no less intrusive way to achieve the same result.

- **Proportionality and Safeguards:** The degree of interference with the individual's right must be proportionate to the public interest sought to be served, and the law must include adequate procedural safeguards to prevent misuse or abuse of power.

Post-Puttaswamy Judicial Engagement

The real-world application of the Puttaswamy principles has been tested through several subsequent challenges.

Puttaswamy II (The Aadhaar Case, 2018)

Commonly referred to as Puttaswamy *II*[15], this 2018 judgment was the first major test of the newly affirmed right to privacy in the context of India's biometric identity program. The Supreme Court was required to determine whether the mandatory collection of biometric data and its centralized storage for welfare delivery violated constitutional guarantees. By a 4:1 majority, the Court upheld the Aadhaar Act as constitutionally valid, reasoning that it served a "legitimate state aim" of ensuring that government subsidies and benefits reached the intended impoverished recipients,. The Court found that the scheme passed the proportionality test because its objective of efficient welfare delivery justified a limited intrusion into informational privacy. Critically, the Court struck down Section 57 of the Aadhaar Act, which had allowed private corporations to use Aadhaar for authentication. The judiciary emphasized that state-mandated data collection must be restricted by strict constitutional limits and cannot be extended to facilitate the commercial interests of private entities without specific legislative backing and safeguards. Justice D.Y. Chandrachud, the lone dissenter, argued that the Aadhaar Act was unconstitutional in its entirety. He raised significant concerns regarding the lack of a robust data protection law at the time, the risks of mass surveillance, and the potential for "data profiling" that could permanently compromise individual autonomy.

2. Digital Access and Communication: *Anuradha Bhasin v. Union of India (2020)*

Following the 2019 communication blackout in Jammu & Kashmir, the Supreme Court addressed the intersection of privacy, free speech, and digital infrastructure in *Anuradha Bhasin*[16]. This case expanded the Puttaswamy framework into the realm of internet access.

> The Court ruled that the freedom of speech and expression under Article 19(1)(a) and the freedom to practice any profession under Article 19(1)(g) both extend to the

[15] (2019) 1 SCC 1
[16] (2020) 3 SCC 637.

internet. It declared that access to digital information is essential for the exercise of modern civil liberties. Applying the proportionality framework, the judiciary held that indefinite or arbitrary internet shutdowns are unconstitutional. The Court mandated that the state must issue public orders for any such restrictions and subject them to periodic judicial and administrative review to ensure they remain "necessary and proportionate" to the stated aim of public order.

3. Surveillance and Accountability: The Pegasus Controversy (2021)

In the case of *Manohar Lal Sharma v. Union of India*[17], the Supreme Court took cognizance of allegations that the state used "Pegasus" spyware to surveil journalists, activists, and political figures.

- **National Security is Not a Blanket Shield:** The Court asserted a vital constitutional principle: the state cannot use "national security" as a "blanket justification" to avoid judicial scrutiny or to infringe upon the privacy of citizens without accountability.
- **The Right to Know:** The judgment reaffirmed that individuals have a right to know if their privacy has been compromised by state surveillance. By forming a technical committee to investigate the spyware allegations, the Court emphasized that procedural safeguards and transparency are mandatory components of a democratic society.

4. Corporate Data Practices: *Karmanya Singh Sareen v. Union of India*[18]

This case brought the focus to the private sector, specifically challenging the data-sharing policies of major messaging platforms like WhatsApp. The litigation raised critical questions about "asymmetrical power structures" between tech giants and user. It pushed for a legal standard where user consent must be "meaningful" and "informed" rather than a procedural formality buried in complex terms of service. The proceedings underscored that informational privacy the right of an individual to control how their data is shared with third parties is a core facet of the right to privacy that requires protection even against non-state actors.

The collective impact of these judgments has been the institutionalization of privacy rights within Indian law. Courts now increasingly view digital identity, surveillance, and data processing through the lens of Article 21, ensuring that any intrusion into an individual's private sphere is backed by law, serves a legitimate purpose, and uses the "least intrusive means"

[17] W.P. (C) No. 314 OF 2021
[18] (2019) 17 SCC 689.

possible. This evolving body of case law serves as the "sentinel on the qui vive," providing the normative standards that the Digital Personal Data Protection (DPDP) Act, 2023 must satisfy to remain constitutionally valid.

IV. Balancing power and privacy: A critical analysis of The Digital Personal Data Protection (DPDP) Act, 2023

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, represents a seminal moment in India's transition toward a regulated digital economy. Following the landmark declaration in *Justice K.S. Puttaswamy Case* that privacy is a fundamental right, the state was placed under a positive obligation to create a statutory framework protecting personal information. This Act is the culmination of years of legislative deliberation, catalyzed by the increasing volume of data processing and the corresponding rise in breaches and misuse. It seeks to balance the individual's right to protect their personal data with the necessity of processing such data for lawful governance and commercial purposes. However, the legislation's practical efficacy depends on its ability to operationalize the constitutional principles of autonomy and dignity within an increasingly digitized society.

The DPDP Act establishes a specific lexicon to define digital data relationships. At its core is personal data, defined broadly as any information that can identify a living individual, either directly or indirectly. The Data Principal is the individual whom the data identifies, while the Data Fiduciary is the entity whether a corporation or government body that determines the purpose and means of processing. This choice of terminology was intended to signify a relationship of trust rather than a mere commercial transaction. To address higher-risk processing, the Act identifies Significant Data Fiduciaries, who are subject to enhanced obligations based on the volume and sensitivity of the data they handle. Additionally, the framework introduces the Consent Manager, a registered entity intended to provide individuals with an accessible interface to manage, withdraw, and track their consent across various platforms.

To empower individuals, the Act grants several enforceable rights that reinforce informational self-determination. The Right to Access Information allows individuals to obtain a summary of their processed data and the identities of other fiduciaries with whom their information was shared. The Right to Correction and Eraser ensures that individuals can rectify inaccuracies or demand the deletion of data that is no longer necessary for its original purpose. Furthermore, the Right of Grievance Redressal mandates that fiduciaries provide a mechanism for

individuals to register complaints before approaching regulatory bodies. In a forward-looking provision, the Right to Nominate allows a principal to appoint a representative to exercise their data rights in the event of death or incapacity. Collectively, these rights are designed to return a degree of control to the individual in an asymmetrical digital environment.

The Act places the primary burden of protection on the Data Fiduciary through a structured Consent Framework. Processing must be based on consent that is "free, specific, informed, unconditional, and unambiguous," signalled by a clear affirmative action. Fiduciaries must adhere to Notice Requirements, providing clear information in multiple languages about the data being collected and the purpose of its use. Substantive obligations include maintaining Security Safeguards to prevent unauthorized access, although the Act has been criticized for leaving the standard of "reasonable" safeguards largely undefined. In the event of a security failure, Data Breach Notification to both the regulator and the affected individuals is mandatory. Specific protections are also mandated for Children's Data, requiring parental consent and prohibiting processing that may cause them harm.

Data Protection Board of India

The Data Protection Board of India (DPBI) is established as the central "watchdog" responsible for enforcing compliance and adjudicating disputes. The Board's composition, consisting of a chairperson and members appointed by the Central Government, has raised significant concerns regarding its institutional independence. Its powers and functions include investigating breaches, issuing directions, and managing a robust penalty framework, where fines for non-compliance can reach up to Rs. 250 crores. While the Board provides a specialized forum for regulatory oversight, critics argue that its close ties to the executive may hamper its ability to impartially adjudicate cases where state agencies themselves are the alleged violators.

Government Exemptions and Executive Discretion

A contentious aspect of the Act is the breadth of statutory exemptions granted to the state under Section 17[19]. The Central Government can exempt its agencies from the Act's provisions on grounds of national security, public order, and public interest. This scope of executive authority allows for large-scale data processing without consent for fulfilling state functions, such as welfare delivery or debt recovery. These provisions raise profound constitutional concerns, as

[19] Digital Data Protection Act, 2023, S 17.

they may insulate government departments from the transparency and accountability measures imposed on private actors. The risk remains that these exemptions could be used as a "blanket justification" to facilitate mass surveillance, potentially contradicting the mandate for narrow tailoring established by the judiciary.

Applying the four-pronged proportionality test from Puttaswamy reveals a complex picture of the Act's constitutional validity. While the Act satisfies the prong of legality by providing a clear legislative basis for data processing, its alignment with the legitimate aim prong is complicated by the breadth of state interests it seeks to serve. The prongs of necessity and proportionality require that state interference be the "least intrusive" possible and narrowly tailored. Critics argue that the Act's sweeping exemptions and the uniform treatment of all data—failing to distinguish highly sensitive categories like health or biometric info—may fail this standard of narrow tailoring. Furthermore, the adequacy of procedural safeguards is questioned given the perceived lack of independence of the Data Protection Board.

Major Criticisms and Implementation Challenges

Significant hurdles persist in the Act's implementation, notably the issue of digital literacy. In a society with varying levels of literacy, consent often becomes a procedural formality rather than a meaningful exercise of autonomy. The prevalence of "dark patterns" interface designs that trick users into sharing more data than intended further undermines the spirit of informed consent. Additionally, the omission of a distinct category for "sensitive personal data" may lead to insufficient safeguards for biometric or financial records. Finally, the heavy reliance on delegated legislation, where many operational details are left to future executive rules, creates compliance uncertainty for businesses and organizations.

The Digital Personal Data Protection Act, 2023, is a transformative development in Indian digital jurisprudence, yet it remains a work in progress. Its success in protecting informational privacy while enabling legitimate state interests will depend on continuous judicial scrutiny to prevent it from becoming a tool for unchecked surveillance. To fulfill the promise of *Puttaswamy*, the judiciary must ensure that state exemptions are interpreted narrowly and that the Data Protection Board operates with genuine institutional integrity. Ultimately, data protection is not merely a regulatory requirement but a constitutional necessity essential for preserving human dignity in the digital age**.**

V. Privacy Promised, Power Preserved? A Critical Evaluation of Section 17 of the Digital Personal Data Protection Act, 2023

While the DPDP Act fills a major regulatory gap, its structure raises significant constitutional and institutional concerns.

Section 17 defines the boundaries of the Act's application by empowering the Central Government to exempt its instrumentalities from the core obligations of data protection. The text allows the State to bypass requirements such as informed consent and individual notice when processing data for specified purposes. These categories of exemptions are broad, encompassing interests such as national security, the sovereignty and integrity of India, public order, and the prevention of offences.

The Government's rationale for these exemptions rests on the exigencies of modern governance. Access to personal data is presented as a prerequisite for efficient welfare delivery, cybersecurity, and law enforcement. By excluding state agencies from certain procedural rigors, the State argues it can more effectively prevent fraud in subsidies and respond to sudden public emergencies or health crises.

The core of data protection jurisprudence lies in the friction between informational privacy the right of an individual to control their personal traces—and the State's legitimate regulatory interests. Privacy functions as a vital constitutional safeguard, shielding individuals from arbitrary State action and psychological coercion. In a democratic society, the processing of data must be transparent to ensure that power is channelled rather than left unchecked. While the DPDP Act seeks to build trust between the "Data Principal" and "Data Fiduciary," the broad exemptions in Section 17 risk creating an "information state" where the individual is increasingly transparent to a state that remains opaque.

To remain constitutionally valid, any state interference with privacy must survive the **four-pronged proportionality test** established in *Puttaswamy*:

- **Legality:** While Section 17 is grounded in an enacted law (the DPDP Act), mere legislative presence is insufficient if the law itself lacks precision.
- **Legitimate State Aim:** National security and welfare are recognized as valid objectives, but the challenge lies in ensuring these aims do not become "blanket justifications" to avoid scrutiny.
- **Necessity and Proportionality:** The *Puttaswamy* framework requires that state measures be **narrowly tailored** and use the "least intrusive means" possible. Critics argue Section 17's wide scope fails this "narrow tailoring" standard, as it treats all

personal data uniformly without distinguishing highly sensitive information like biometric or health records.

- **Procedural Safeguards:** The Act's reliance on a **Data Protection Board** appointed and controlled by the Central Government raises concerns that there is no independent oversight to check the misuse of these exemptions.

The breadth of Section 17 invites significant concerns regarding excessive executive discretion. Because many operational details are delegated to future rules and government notifications, the executive maintains substantial authority to define the "public interest" unilaterally. Scholars and civil society organizations have warned that this lack of independent regulatory oversight could legitimize mass surveillance and data-sharing practices that bypass constitutional guardrails. Without robust accountability mechanisms, informational privacy may be sacrificed at the altar of administrative convenience.

Comparative Perspective

When compared to the European Union's General Data Protection Regulation (GDPR), the Indian framework reveals a concerning tilt toward the State. The GDPR insists on independent supervisory authorities that are strictly insulated from political influence. While the GDPR also allows for exemptions in the interest of national security, it embeds much stronger principles of transparency, purpose limitation, and individual rights than the current Indian regime. Consequently, India's approach provides arguably weaker privacy protections by granting the government wider discretion without equivalent independent checks.

The debate over Section 17 reflects a shift from "rights-maximalism" toward regulatory pragmatism. Supporters argue that these powers are necessary for a developing nation to ensure security and social welfare. However, critics contend that the Act disproportionately favors State power, potentially reducing fundamental rights to a procedural formality. By creating a "rights-and-duties" model that imposes obligations on citizens while granting "blanket" exemptions to the State, the Act risks undoing the individual-centric vision of the *Puttaswamy* judgment.

VI. Suggestions and Recommendations

The transition from the constitutional recognition of privacy in Justice K.S. Puttaswamy case to the statutory implementation under the Digital Personal Data Protection (DPDP) Act, 2023, underscores a persistent tension between individual autonomy and state authority. While the

Act provides a long-awaited regulatory structure, its current form reflects a "regulatory pragmatism" that prioritizes administrative ease over the rigorous standards of necessity and proportionality established by the Supreme Court. To harmonize this framework with the spirit of the *Puttaswamy* judgment, specific, evidence-based reforms are required to recalibrate the balance of power.

Central to this recalibration is the need to narrowly interpret and reform the broad state exemptions granted under Section 17 of the Act. In its present iteration, the Central Government possesses the authority to exempt its agencies from the Act's core obligations on expansive grounds such as national security, public order, and the prevention of offences. To meet the constitutional requirement of "narrow tailoring," these exemptions must be subjected to periodic judicial or parliamentary review rather than remaining as blanket justifications for data processing. The state's legitimate interests in national security and public administration should not serve as an opaque shield against accountability; instead, any intrusion must be proven to be the "least intrusive means" available to achieve a specific, legitimate goal.

Furthermore, the institutional integrity of the Data Protection Board of India (DPBI) must be fortified through greater independence from executive influence. Unlike the independent supervisory authorities mandated under the EU's General Data Protection Regulation (GDPR), which are strictly insulated from political control, the DPBI is largely constituted and controlled by the Central Government. This structural dependency raises concerns regarding the Board's capacity to impartially adjudicate disputes where the state itself is a Data Fiduciary. Reforms should include a transparent, merit-based appointment process for Board members and a secure tenure that prevents arbitrary removal by the executive, thereby ensuring that the "watchdog" can effectively bark at the hand that feeds it.

To prevent arbitrary state access to personal data, the framework must incorporate more robust procedural safeguards and transparency mechanisms. This includes the mandatory requirement for Data Protection Impact Assessments (DPIAs) for state-led processing activities involving sensitive information, as well as strengthening individual rights of access and correction. Drawing lessons from the GDPR, the Indian law should progressively recognize the "right to data portability" and the "right to be forgotten," which were present in earlier drafts but omitted from the final Act. These rights are essential for maintaining informational self-determination in an age of asymmetrical power structures.

Another critical area for reform is the reintroduction of a risk-based category for "sensitive personal data". The current Act's uniform treatment of all personal data fails to distinguish between relatively innocuous information and highly sensitive categories like health, financial, or biometric records. By re-establishing this distinction, the law can impose stricter security obligations and higher standards of consent for the processing of data that poses a greater risk to human dignity.

Finally, for these statutory rights to be meaningful, the state must tackle the structural challenges of digital literacy and the prevalence of "dark patterns". Consent interfaces should be legally mandated to be clear, concise, and available in regional languages to ensure that the "Data Principal" is exercising meaningful autonomy rather than merely fulfilling a procedural formality. The judiciary must continue to act as the "sentinel on the qui vive," applying the proportionality test to ensure that the "new oil" of data is processed within a framework that respects the fundamental rights of every Indian citizen. Ultimately, the success of India's data protection regime depends on shifting the regulatory culture to view privacy not as a compliance burden, but as an essential component of democratic governance.

VII. Conclusion

The critical examination of India's evolving data protection landscape reveals a profound transformation in the constitutional relationship between the individual, the state, and the digital economy. This study began by addressing the central tension of our era: the dual nature of personal data as both the "lifeblood" of modern governance and a potential vector for unprecedented harm. At the heart of this research was the question of whether the Digital Personal Data Protection (DPDP) Act, 2023, succeeds in operationalizing the visionary standards of informational privacy established by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India.

The constitutional significance of the *Puttaswamy* judgment cannot be overstated. By unanimously declaring privacy a fundamental right under Article 21, the Court dismantled the "isolated silos" doctrine that had long constrained Indian jurisprudence. The judgment moved beyond a mere "animal existence" interpretation of life to one defined by dignity, autonomy, and the "inner recesses of the human personality". Most critically, it established informational privacy the right of an individual to control the dissemination of their digital traces as a core attribute of personhood in the 21st century. Through the articulation of the four-pronged

proportionality test legality, legitimate aim, necessity, and procedural safeguard the Court provided a robust benchmark against which all future state intrusions must be measured.

The findings of this study suggest that the DPDP Act, 2023, reflects these principles in its foundational intent but frequently departs from them in its structural implementation. On one hand, the Act fills a decades-old legislative vacuum, providing a nationwide framework for digital data processing and establishing the individual as a "Data Principal" endowed with enforceable rights. The introduction of massive monetary penalties and the creation of the Data Protection Board of India (DPBI) signal a legislative desire to build a "trusted shield" for India's secure digital future.

However, a critical assessment of the Act reveals a significant shift from "rights-maximalism" toward "regulatory pragmatism". Unlike the EU's GDPR, which offers a broader catalogue of rights, the Indian regime omits robust versions of the "right to data portability" and the "right to be forgotten" found in earlier drafts. Furthermore, by adopting a uniform treatment for all personal data, the Act fails to distinguish highly sensitive categories such as biometric, health, or financial information that inherently require higher standards of security and consent.

The most contentious threat to the privacy–power balance lies in Section 17 and the broad state exemptions. While the state has legitimate objectives in national security and welfare delivery, the breadth of these provisions' risks violating the *Puttaswamy* mandate for "narrow tailoring". By allowing the Central Government to exempt its agencies from core obligations, the Act risks creating an "information state" where the government remains opaque while the citizen is made increasingly transparent. This imbalance is compounded by concerns regarding the institutional independence of the DPBI, which, unlike independent authorities in other jurisdictions, remains under the administrative and appointive control of the executive.

This research highlights that while the Act empowers individuals in theory, informational self-determination is hindered by practical realities. In a society with limited digital literacy, the "consent framework" often collapses into a procedural formality. The prevalence of "dark patterns" and the structural asymmetry between large tech fiduciaries and ordinary citizens suggest that consent alone is an insufficient guardrail for privacy.

Several constitutional challenges remain unresolved. The Act remains silent on the comprehensive regulation of state surveillance, a gap brought into sharp relief by the *Pegasus* controversy and the internet shutdowns explored in *Anuradha Bhasin*. The judiciary's ongoing role as the "sentinel on the qui vive" is therefore essential. The true effectiveness of India's

regime will depend not on the text of the law, but on how courts interpret state exemptions and the degree to which the DPBI can operate with genuine institutional integrity.

In the final assessment, the DPDP Act is a landmark achievement, but it represents the beginning of a journey rather than a final destination. To truly fulfill the *Puttaswamy* promise, the regime must move toward a more nuanced categorization of sensitive data, a narrowing of state exemptions to meet the "least intrusive means" standard, and a commitment to regulatory independence.

As India marches further into a data-driven era, its constitutional democracy must ensure that privacy is not treated as an obstacle to development but as its very prerequisite. The digital landscape is in a state of flux, shaped by emerging technologies that the framers of the Constitution could not have foreseen. Nevertheless, the principles of dignity, autonomy, and the rule of law remain eternal. The future of privacy in India hinges on the state’s ability to view data protection not as a compliance burden, but as a vital component of human dignity. In this grand constitutional project, the individual must remain the master of their own digital destiny, ensuring that the "new oil" of data is used to fuel progress without incinerating the fundamental right to be let alone.