JUDICIAL INTERPRETATION AND DATA RIGHTS IN INDIA: FROM PUTTASWAMY TO THE DPDP ACT, 2023

Dr. Kuldeep Singh Panwar, HOD, Associate Professor, Department of Law, Nagaland University, Lumami

Jaishree Gaur, Research Scholar, Department of Law, Nagaland University, Lumami

ABSTRACT

This article explores the evolving landscape of data rights in India, focusing on the judicial interpretation of privacy rights from the Puttaswamy judgment to the enactment of the Digital Personal Data Protection (DPDP) Act, 2023. The Puttaswamy case laid the constitutional foundation for the recognition of the right to privacy as a fundamental right under Article 21, emphasizing autonomy, dignity, and informed consent. Building on this foundation, the DPDP Act seeks to regulate the collection, processing, and storage of personal data, with a focus on balancing privacy with state interests in national security, law enforcement, and public welfare. Key features of the Act, such as consent frameworks, the rights of data principals, and government exemptions, are critically analyzed in light of constitutional principles, including proportionality and necessity. The article further discusses the potential role of the judiciary in interpreting and enforcing the Act's provisions, with particular attention to emerging challenges such as government surveillance and lack of independent regulatory oversight. The paper concludes that while the DPDP Act represents progress in data protection, its implementation and future development will depend on ongoing judicial scrutiny to ensure a balance between privacy and public interest in an increasingly digitized society.

Keywords: Data Protection, Right to Privacy, Puttaswamy Judgment, Digital Personal Data Protection (DPDP) Act, Judicial Interpretation, Proportionality Principle

1. Introduction

In the digital era, personal data has emerged as both a valuable asset and a potential vector of harm. With the exponential growth in digital communication, e-governance, fintech, and surveillance technologies, the protection of personal data has become an essential component of democratic governance. Data rights, especially the right to informational privacy, have gained prominence not only in academic discourse but also in public consciousness. These rights are no longer limited to concerns of secrecy or intrusion but extend to issues of autonomy, consent, data localization, and algorithmic governance.

The Indian legal landscape has witnessed a paradigm shift in how data rights are understood and protected. This transformation began with the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where the Supreme Court unanimously affirmed the right to privacy as a fundamental right under the Constitution of India. The judgment laid the constitutional foundation for the development of data protection norms by explicitly recognizing the need for legal safeguards against state and non-state actors in the digital age.

Judicial interpretation has played a pivotal role in shaping the contours of privacy jurisprudence in India. Through progressive rulings, the judiciary has delineated the parameters within which individual rights must be respected and protected, even in the face of competing interests such as national security, public order, and economic development. The introduction of the proportionality principle in *Puttaswamy* has further enriched this discourse by offering a structured framework for balancing individual rights with legitimate state objectives.

This article aims to explore the evolution of judicial thought on data rights in India, beginning with the *Puttaswamy* judgment and extending to the contemporary statutory response in the form of the Digital Personal Data Protection (DPDP) Act, 2023. It examines how the judiciary has influenced the development of privacy and data protection norms and how future interpretations may shape the enforcement and scope of the DPDP Act.

Scope and Objectives:

- To trace the constitutional recognition and judicial development of the right to privacy in India.
- To analyze key judicial decisions post-*Puttaswamy* that have contributed to the discourse on data rights.

- To evaluate the extent to which the DPDP Act aligns with constitutional principles laid down by the judiciary.
- To assess the potential role of judicial review in interpreting and enforcing the DPDP Act in the future.

In doing so, the article contributes to a broader understanding of the symbiotic relationship between constitutional law and statutory evolution in the context of digital rights and governance.

2. The Constitutional Foundation of Data Rights: Puttaswamy Judgment

The landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) marked a watershed moment in the evolution of constitutional rights in India. It laid down the foundational jurisprudence for data rights by elevating the right to privacy to the status of a fundamental right. The case not only redefined the contours of Article 21 but also introduced judicial tools like the proportionality principle to evaluate the reasonableness of state action involving individual rights. In doing so, it set the stage for a rights-based framework for data protection and digital governance in India.

2.1 Background of the Puttaswamy Case

The *Puttaswamy* case arose in the context of a broader challenge to the constitutionality of the Aadhaar scheme, India's biometric-based identity program. Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a petition before the Supreme Court in 2012, arguing that the Aadhaar program—by mandating the collection and storage of sensitive personal data without legislative backing—violated the right to privacy of individuals.

The Union Government, however, contested the existence of a fundamental right to privacy under the Indian Constitution. It relied on earlier rulings such as *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962), where privacy had not been recognized as a fundamental right. This divergence of judicial opinion over decades prompted the Supreme Court to constitute a nine-judge constitutional bench to resolve the question: **Is the right to privacy a fundamental right under the Constitution of India?**

The petitioners argued that privacy is intrinsic to the right to life and personal liberty under Article 21, and also flows from other rights such as freedom of expression (Article 19(1)(a)), freedom of movement (Article 19(1)(d)), and the right to freedom of religion (Article 25). The

case thus became a platform for a deeper philosophical and legal inquiry into the meaning of privacy in the digital age.

2.2 Recognition of the Right to Privacy as a Fundamental Right

In a historic and unanimous decision in August 2017, the Supreme Court held that the right to privacy is a constitutionally protected fundamental right, emanating primarily from Article 21, but also intersecting with various other fundamental freedoms. The judgment was authored by a plurality of justices, each contributing different facets of privacy, such as bodily integrity, informational self-determination, decisional autonomy, and dignity.

Three central constitutional values were emphasized:

- **Autonomy**: The right to privacy empowers individuals to make personal choices without unwarranted interference by the state or other entities. This includes the right to make decisions about one's body, sexuality, and personal relationships.
- **Dignity**: The Court held that privacy is essential to the preservation of human dignity. Any intrusion into one's private space—be it through surveillance, data collection, or behavioral profiling—impinges on their self-respect and personhood.
- **Consent**: A key theme of the judgment was that consent forms the ethical basis for any access to personal information. Informational privacy was seen as the individual's ability to control the dissemination of personal data.

Justice Chandrachud, writing for the majority, noted that "informational privacy" is particularly relevant in the digital age where individuals routinely share data with service providers, often under asymmetrical power structures and unclear consent mechanisms.

By recognizing the right to privacy as fundamental, the Court imposed a duty upon the state to ensure that any law or executive action that limits privacy must meet constitutional standards. This had far-reaching consequences, especially for India's nascent data protection regime.

2.3 Introduction of the Proportionality Principle

One of the most critical legal tools articulated in *Puttaswamy* was the **proportionality test**, which serves as a balancing mechanism to assess whether restrictions on fundamental rights are constitutionally valid. This doctrine has since become a cornerstone of Indian constitutional law in privacy-related jurisprudence.

The proportionality principle involves four prongs:

1. **Legality**: There must be a law that sanctions the state's action infringing on privacy. Executive or administrative discretion alone is insufficient.
2. **Legitimate Aim**: The restriction must pursue a legitimate state interest—such as national security, prevention of crime, or protection of health.
3. **Necessity**: The means employed must be necessary and not arbitrary; there should be no less intrusive way of achieving the same objective.
4. **Proportionality**: The degree of interference with the right must be proportionate to the public interest sought to be achieved.
5. **Procedural Safeguards** *(as evolved in subsequent cases)*: There must be adequate safeguards to prevent abuse, including oversight mechanisms and remedies for aggrieved individuals.

The adoption of this test places a significant burden on the state to justify any law or action that affects the informational privacy of individuals. It also offers a framework for future judicial review of data-centric legislations and policies.

The *Puttaswamy* judgment thus does not merely declare privacy as a right—it actively **operationalizes** it by providing a legal standard against which all intrusions into personal and data privacy must be measured.

3. Expansion of Judicial Interpretation: Post-Puttaswamy Case Law

The *Puttaswamy* verdict laid a powerful constitutional foundation, but the real test of its effectiveness has been in its application. In the years that followed, Indian courts have grappled with applying the principles laid down in *Puttaswamy* to a range of real-world challenges involving surveillance, digital identity, internet restrictions, and privacy violations. This evolving jurisprudence reflects the judiciary's engagement with balancing individual privacy with legitimate state objectives such as welfare, national security, and technological advancement.

3.1 Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018)

Shortly after the 2017 verdict, the Supreme Court delivered its judgment on the constitutional validity of the Aadhaar program in *Justice K.S. Puttaswamy (Aadhaar) v. Union of India*

(2018), often referred to as *Puttaswamy II*.

Key Issues and the Balancing Act

The core question was whether the Aadhaar scheme—which involved biometric authentication and centralized data storage—violated the right to privacy. Petitioners raised concerns over mass surveillance, data profiling, exclusion from welfare schemes due to authentication failures, and the lack of a robust data protection law.

The Court, by a 4:1 majority, upheld the Aadhaar Act as constitutionally valid, but with significant caveats. It struck down several provisions that allowed Aadhaar to be used by private entities and limited its use to welfare schemes backed by legislation. The Court reasoned that the Aadhaar project served a legitimate state aim—ensuring targeted delivery of subsidies and benefits—and passed the proportionality test laid down in *Puttaswamy I*.

Privacy Safeguards and Limitations

While the majority emphasized procedural safeguards, Justice D.Y. Chandrachud's dissent took a more privacy-centric view, declaring the Aadhaar Act unconstitutional in its entirety for failing to meet procedural and substantive due process requirements. His dissent raised concerns over lack of data minimization, absence of data protection legislation, and the possibility of state surveillance.

The judgment marked the judiciary's attempt to strike a balance between welfare and surveillance, setting a precedent that welfare objectives can justify certain intrusions into privacy—but only within strict constitutional limits.

3.2 Internet Freedom and Surveillance

Post-*Puttaswamy*, the Indian judiciary has dealt with several cases concerning state surveillance, internet shutdowns, and the right to free expression in the digital space. These cases illustrate the expanding relevance of privacy jurisprudence in a technologically mediated public sphere.

a. Anuradha Bhasin v. Union of India (2020)

In the wake of the abrogation of Article 370 in Jammu & Kashmir, the government imposed a communication blackout, including a complete internet shutdown. In *Anuradha Bhasin v. Union of India*, the Supreme Court examined whether such restrictions violated fundamental rights.

The Court held that freedom of speech and expression under Article 19(1)(a) and freedom of trade and commerce under Article 19(1)(g) extended to the internet. It emphasized that restrictions on internet access must be proportionate, legal, and subject to judicial review. The ruling reinforced the proportionality framework laid down in *Puttaswamy*, recognizing that indefinite or arbitrary internet shutdowns could not be justified under the guise of public order.

Though the Court stopped short of lifting the shutdown, it mandated periodic review and publication of shutdown orders, setting a standard for future actions.

b. Pegasus Spyware Controversy

In 2021, allegations emerged that Pegasus spyware—developed by the Israeli NSO Group—was used to surveil Indian citizens, including journalists, activists, and politicians. In *Manohar Lal Sharma v. Union of India* and related petitions, the Supreme Court took suo motu cognizance.

A significant outcome was the formation of a technical committee to probe the allegations, with the Court asserting that the state cannot use national security as a blanket justification to avoid judicial scrutiny. The Court reaffirmed that citizens have a right to know whether their privacy has been compromised and emphasized accountability, transparency, and procedural safeguards.

While the final findings of the committee were inconclusive, the proceedings underscored that judicial oversight is necessary even in matters of surveillance—a direct application of *Puttaswamy's* proportionality doctrine.

3.3 Emerging Trends and Observations

The post-*Puttaswamy* period has revealed several important trends in judicial interpretation:

- **Institutionalizing Privacy Rights**

  Indian courts are now more inclined to examine issues involving surveillance, internet regulation, and personal data collection through the lens of privacy rights. There is an increasing tendency to apply the **four-part proportionality test**, ensuring that intrusions are justified, necessary, and procedurally sound.

- **Expansion Beyond Article 21**

  The courts are increasingly recognizing that data rights are not limited to Article 21. They

intersect with freedom of expression (Article 19), equality (Article 14), and even freedom of profession (Article 19(1)(g)) in the context of digital businesses and economic activity.

- **Judicial Reluctance vs. Assertiveness**

While the judiciary has shown willingness to engage with digital rights, there remains a degree of judicial restraint in challenging state actions on surveillance and national security grounds. Cases like *Anuradha Bhasin* and *Pegasus* reflect a cautious but increasingly assertive judiciary, seeking transparency without compromising the state's legitimate concerns.

- **Anticipatory Engagement with Legislation**

As the Digital Personal Data Protection (DPDP) Act, 2023, comes into force, courts are expected to play a critical role in **interpreting its provisions in light of the constitutional principles laid down in *Puttaswamy*.** Early challenges to exemptions, regulatory gaps, and enforcement mechanisms are likely to shape the operational landscape of the Act.

4. Statutory Response and the DPDP Act, 2023

The *Puttaswamy* judgment marked a constitutional milestone by affirming the right to privacy as a fundamental right under Article 21 of the Indian Constitution. While this judgment laid the constitutional groundwork, it also underscored the urgent need for a comprehensive legislative framework to protect personal data. The vacuum in statutory protections and the increasing digitization of governance and commercial services prompted the Indian state to initiate a legislative response, eventually culminating in the **Digital Personal Data Protection Act, 2023 (DPDP Act)**. This Act represents India's first focused legislative attempt to regulate the processing of digital personal data, balance privacy with state and business interests, and establish a statutory data protection authority.

4.1 Legislative Journey Post-Puttaswamy

The judicial recognition of privacy in 2017 served as the catalyst for legislative action. Soon after the *Puttaswamy* judgment, the central government set up the **Justice B.N. Srikrishna Committee** to deliberate on data protection concerns and propose a legal framework. In 2018, the committee submitted a comprehensive report along with a draft Personal Data Protection Bill. The report emphasized that privacy is an essential facet of individual autonomy and dignity, and any data protection law must be rights-centric, grounded in informed consent, and

subject to independent oversight.

In 2019, the government introduced a revised version of this draft—the Personal Data Protection Bill, 2019—in Parliament. However, this version attracted considerable criticism for diluting user rights, granting excessive exemptions to government agencies, and establishing a central authority heavily under executive control. Due to these concerns, the Bill was eventually withdrawn in August 2022. In its place, a simplified and business-friendly **Digital Personal Data Protection Bill, 2022** was introduced, which was passed by Parliament in 2023 as the **DPDP Act**. Unlike its predecessor, the 2023 Act reflects a shift towards regulatory pragmatism, emphasizing ease of compliance over rights-maximalism.

4.2 Key Features of the DPDP Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023 is a landmark legislation that establishes the foundational framework for the governance of personal data in India. The Act incorporates essential elements such as extraterritorial applicability, a consent-based processing model, data principal rights, fiduciary obligations, institutional oversight, and government exemptions. Each of these features reflects the intent to strike a balance between privacy protection, ease of doing business, and national interests.

Applicability and Jurisdiction

The DPDP Act has both territorial and extraterritorial applicability. It governs the processing of digital personal data collected within India, whether obtained directly in digital form or initially collected offline and later digitized. Importantly, the Act also applies to data processing conducted outside India if it pertains to offering goods or services to individuals located in India. This provision aligns India’s law with global standards such as the EU's General Data Protection Regulation (GDPR), enabling broader jurisdictional reach in a digitally interconnected world.

Consent-Based Processing and Legitimate Use

At the heart of the DPDP Act lies a consent-driven framework. Personal data may be processed only for lawful purposes and with the informed, specific, and unambiguous consent of the data principal. Before seeking consent, data fiduciaries are obligated to furnish clear notice outlining the purpose of data collection and intended usage.

However, the Act also introduces the concept of "legitimate use", where data can be processed

without explicit consent in limited scenarios. These include processing necessary for state functions, legal obligations, public interest, or during emergencies such as natural disasters and health crises. While these exceptions offer operational flexibility, they have been criticized for potentially diluting the centrality of consent and creating space for unchecked data processing, especially by state actors.

Rights of Data Principals

The DPDP Act endows individuals, referred to as data principals, with certain enforceable rights over their personal data. These include the right to access information regarding data processing, the right to correction and erasure of inaccurate or unnecessary data, and the right to grievance redressal in case of violations. These rights are intended to empower individuals and reinforce informational autonomy.

However, notable rights such as the right to data portability and the right to be forgotten, which were proposed in earlier drafts of the law, have been omitted in the final version. This has raised concerns regarding the Act's alignment with international privacy norms and its ability to offer a comprehensive suite of user protections.

Obligations of Data Fiduciaries

The DPDP Act imposes several responsibilities on data fiduciaries, i.e., the entities that determine the purpose and means of data processing. They are required to ensure data security, prevent unauthorized access or misuse, and report data breaches to both the Data Protection Board of India and affected individuals.

Moreover, the Act introduces the category of Significant Data Fiduciaries—entities that process large volumes or sensitive types of personal data. These fiduciaries are subject to enhanced obligations, such as appointing Data Protection Officers, conducting Data Protection Impact Assessments (DPIAs), and maintaining higher compliance standards. This classification is designed to manage risks proportionate to the scale and sensitivity of data handling.

The Data Protection Board of India

The Data Protection Board of India serves as the enforcement and adjudicatory body under the DPDP Act. It is tasked with monitoring compliance, handling disputes, and imposing penalties in cases of data breaches or non-compliance. However, the independence and autonomy of the

Board have been questioned. Unlike independent data protection authorities in jurisdictions such as the EU or UK, the Indian Board is constituted and controlled by the central government, raising concerns over potential executive interference and the dilution of accountability mechanisms.

Government Exemptions under Section 17

One of the most contentious aspects of the DPDP Act is Section 17, which empowers the central government to exempt any of its agencies from compliance with the Act for reasons including national security, sovereignty, public order, and foreign relations. These exemptions are broadly framed and lack adequate procedural safeguards, prompting fears that they may be used to legitimize mass surveillance or avoid transparency. Critics argue that such unqualified exemptions contradict the proportionality doctrine emphasized in the *Puttaswamy* judgment and threaten the very privacy protections the Act purports to safeguard.

4.3 Alignment with Constitutional Principles

The DPDP Act attempts to operationalize several constitutional values recognized in *Puttaswamy*, such as individual autonomy, informed consent, and privacy. However, it does so through a minimalist approach that prioritizes simplification and business facilitation over a comprehensive rights-based regime. For example, unlike the earlier drafts that categorized personal data into sensitive, critical, and general categories requiring different levels of protection, the DPDP Act adopts a uniform treatment of all personal data, which may fail to account for the varying levels of privacy sensitivity.

The Act's design reflects a trust-based governance model, assuming voluntary compliance and responsible behavior from data fiduciaries. However, this could undermine individual empowerment in contexts where asymmetries of power and information persist—especially between large tech corporations and ordinary citizens. Moreover, the absence of strong independent oversight mechanisms weakens the constitutional guardrails that the Supreme Court sought to establish.

4.4 Challenges and the Road Ahead

As India moves into the implementation phase of the DPDP Act, several critical challenges remain. First, the Act's constitutional validity is likely to be tested before the judiciary. Questions may arise around whether Section 17's government exemptions violate the *Puttaswamy* proportionality test and whether the Data Protection Board's lack of independence

infringes upon the right to an effective remedy. These issues will require careful judicial scrutiny and may result in further interpretative evolution of the Act.

Second, the Act must function within a broader legal and regulatory ecosystem. It will intersect with existing frameworks such as the Information Technology Act, 2000, criminal provisions on data theft and cybercrime, and sectoral laws like those governing finance and health. Additionally, proposed legislations like the Digital India Act will further impact its scope and implementation. Harmonizing these overlapping regimes is essential to prevent confusion and ensure cohesive enforcement.

Finally, successful implementation will require significant institutional and public capacity-building. Many data fiduciaries, especially smaller entities and government departments, may lack the resources and technical capacity to comply. Awareness among citizens about their rights under the Act is also limited. The effectiveness of the DPDP Act will depend on training, **digital literacy, public outreach**, and the empowerment of data principals to assert their privacy rights.

5. Judicial Implications and the Way Forward

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, has significant implications for the Indian judiciary. As the law begins to be operationalized, courts will play a crucial role in interpreting its provisions, resolving conflicts, and ensuring its alignment with the constitutional principles laid down in *Puttaswamy* and subsequent decisions. This section explores the anticipated role of the judiciary under the new legal regime, emerging interpretive challenges, and the broader path ahead for privacy jurisprudence in India.

5.1 Role of Judiciary in Interpreting the DPDP Act

The Indian judiciary has historically acted as the guardian of fundamental rights, especially in the context of evolving technologies and civil liberties. With the DPDP Act now in force, courts will likely be called upon to interpret key statutory concepts such as “consent,” “legitimate use,” “public interest,” and “data fiduciary obligations.” Given the vague and broadly worded provisions in several parts of the Act, especially concerning exemptions for government agencies, the judiciary will need to clarify legislative intent and ensure that executive action remains within the constitutional limits of proportionality and necessity.

Moreover, courts will have to determine how the DPDP Act coexists with other statutes such as the Information Technology Act, 2000, and sectoral regulations (e.g., in finance, telecom,

or healthcare). This interpretive role will be central to shaping the Act's practical enforcement and harmonizing India's data governance framework.

5.2 Challenges in Balancing Privacy and State Interests

A recurring tension in data protection law lies in balancing individual privacy rights with the state's interests in national security, law enforcement, and public welfare. The DPDP Act explicitly authorizes the state to process personal data without consent for specified "legitimate uses" and grants itself sweeping exemptions under Section 17.

The judiciary will face the complex task of examining whether such actions satisfy the Puttaswamy proportionality test, which requires legality, legitimate purpose, necessity, and procedural safeguards. Courts must critically examine whether such exemptions are narrowly tailored and backed by adequate oversight mechanisms. Failure to do so could undermine the very foundation of informational privacy, setting a precedent for unchecked surveillance or misuse of data under the guise of public interest.

5.3 Potential for Judicial Review and Constitutional Scrutiny

Given the contentious nature of certain provisions—especially those relating to government exemptions, lack of independent oversight, and absence of certain data principal rights—it is foreseeable that the DPDP Act may be challenged before constitutional courts. Petitioners could argue that the Act violates the right to privacy under Article 21, fails to meet the standards of procedural fairness, and creates disproportionate limitations on fundamental rights.

Judicial review of the DPDP Act would also provide an opportunity to test the scope and enforceability of digital rights in India. It could lead to the development of a richer body of jurisprudence on data protection, helping courts define the contours of privacy in the digital age and reinforcing the normative standards established in *Puttaswamy*.

5.4 The Road Ahead: Harmonizing Rights and Regulation

Moving forward, India's legal and judicial systems must work in tandem to strengthen the privacy regime. This includes ensuring that future data protection jurisprudence reflects a rights-based approach, especially in areas such as algorithmic accountability, automated decision-making, and cross-border data transfers. Courts may also be called upon to develop interim safeguards in the absence of comprehensive rules or when the executive delays in setting up mechanisms like the Data Protection Board.

Ultimately, the judiciary must act as a check on potential executive overreach, uphold the principles of transparency and accountability, and ensure that privacy is not sacrificed at the altar of convenience or control. The real test will lie not just in statutory interpretation but in how effectively the courts internalize constitutional values while navigating the complexities of the digital era.

Conclusion

The evolution of data rights in India, from the landmark *Puttaswamy* judgment to the enactment of the DPDP Act, 2023, reflects a broader global trend towards securing privacy in the face of rapid technological advancement. While the *Puttaswamy* decision laid a firm foundation by recognizing the right to privacy as a fundamental right under Article 21, it also set the stage for legislative reforms in response to the digital age. The DPDP Act, by establishing a legal framework for personal data protection, attempts to balance the interests of privacy with the practical needs of economic and technological growth.

However, the Act's implementation raises several important questions, particularly regarding the role of consent, the legitimacy of government exemptions, and the need for independent regulatory oversight. The judiciary will continue to play an essential role in shaping the interpretation of these provisions, ensuring that the Act upholds the constitutional guarantees of autonomy, dignity, and accountability. The Puttaswamy framework, with its emphasis on the proportionality principle, will be crucial in resolving these challenges and safeguarding individual privacy in a rapidly evolving digital landscape.

In conclusion, while the DPDP Act represents a significant step forward in the protection of personal data in India, it is only through the continued judicial engagement and constitutional scrutiny that the law will reach its full potential. The courts must ensure that the Act does not become a tool for unchecked surveillance but rather functions as a robust shield protecting individuals' rights in the digital era. The future of data protection in India hinges on the ability of the judiciary to navigate the complex intersection of privacy, technology, and state power, ensuring that data governance evolves in a way that respects both individual rights and public welfare.

References

1. Anirudh Burman, *Understanding India's New Data Protection Law*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 3, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.
2. Tanmay Singh & Gayatri Malhotra, *The Digital Personal Data Protection Bill, 2022 Does Not Satisfy the Supreme Court's Puttaswamy Principles*, INTERNET FREEDOM FOUND. (Dec. 16, 2022), https://internetfreedom.in/the-digital-personal-data-protection-bill-2022-does-not-satisfy-the-supreme-courts-puttaswamy-principles/.
3. Anandan S, *India's Digital Data Protection Act 2023: Key Insights and Comparisons with GDPR*, DE PENNING & DE PENNING (Mar. 5, 2025).
4. Raktima Roy & Gabriela Zanfir-Fortuna, *The Digital Personal Data Protection Act of India, Explained*, FUTURE PRIVACY F. (Aug. 15, 2023), https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.
5. Vajiram Editor, *Right to Privacy: Evolution, Significance, Challenges*, VAJIRAM & RAVI (Jan. 27, 2025), https://vajiramandravi.com/upsc-exam/right-to-privacy/.
6. Chris Brook, *What is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know*, DIGITAL GUARDIAN (June 28, 2023), https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you.