IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# Right to Privacy In India: From KS Puttaswamy to The Digital Personal Data Protection Act, 2023

BY

**Nidhi Thakur***
**nidhi.thakur1424@gmail.com**
RESEARCH SCHOLAR
DEPARTMENT OF LAW
HIMACHAL PRADESH UNIVERSITY, SHIMLA (HP)

**DR. Rajinder Verma**
**rajinder.law@hpuniv.ac.in**
PROFESSOR
DEPARTMENT OF LAW
HIMACHAL PRADESH UNIVERSITY, SHIMLA (HP)

**ABSTRACT**

In a time of unparalleled digital data explosion and unrelenting technological advancement, protecting personal information has emerged as a top priority for people, businesses, and governments everywhere. Due to global digitization, especially in India, the significance of data protection has increased dramatically over the last few decades, reaching previously unthinkable heights. The concept of "privacy" has existed since the dawn of human civilization. However, it could be difficult to comprehend privacy. Scholars cannot agree on a single definition of "privacy" because the idea changes as society does. Over the course of human history, the phrase "right to privacy" has expanded to encompass rights like the right to anonymity or the right to be left alone. Given the widespread usage of digital media in today's world, protecting this freedom is essential. The implementation of the Digital Personal Data Protection Act, 2023, is significant because it creates guidelines for the legitimate processing of personal data, giving authorities and protecting persons' rights.

Keywords: Privacy, data protection, digital, personal data

## Introduction:

Human rights should be universal, inviolable and inherent in every human being. ''PRIVACY'', as the most valuable human right of all, is protected in several important regional, national, and international instruments.

The right to privacy which is an important part of one's life and personal liberty plays a significant role in the development of one's personality, integrity and dignity.[1]The UN Declaration of Human Rights, European Convention on Human Rights and many other International and Regional treaties recognizes privacy as a fundamental human right. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issue of modern age.[2]

In India, the expansion of the right to privacy has been one of the most significant legal advances in recent years. The journey of recognizing and enforcing the right to privacy has taken a significant turn, beginning with a landmark judicial decision in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) and culminating in the enactment of the Digital Personal Data Protection Act, 2023. This tendency reflects an increasing awareness of informational privacy, autonomy, and the necessity for legislative safeguards in an age of widespread digital surveillance and data monetization.

The Supreme Court's decision in the Puttaswamy case was a landmark moment in constitutional history, establishing the right to privacy as a basic right under Article 21 of the Indian Constitution. The ruling underlined that privacy encompasses not just physical and decisional liberty, but also informational self-determination, setting the groundwork for a comprehensive data protection framework.

To fill the gap in the current legal protections, the Indian government started the process of creating a data protection law after the Puttaswamy ruling. The initial draft of a data protection bill was created in 2018 based on the suggestions of the Justice B.N. Srikrishna Committee, and it has since undergone further revisions. The Digital Personal Data Protection Act (DPDP Act), 2023, which was finally approved after a number of discussions, modifications, and consultations, represents India's official legislative answer to the issues raised by the digital economy.

The DPDP Act is a historic law because it embodies fundamental ideas like accountability, purpose limitation, consent-based data collection, and data minimization. It also reflects local concerns and administrative capabilities while bringing India's approach into compliance with international norms like the EU's General Data Protection Regulation (GDPR)[3].

Therefore, the path from Puttaswamy to the DPDP Act is more than just a change in the law; it marks India's shift from a legal framework that recognized privacy to a legally binding system that protects personal information. Ensuring dignity, freedom, and democratic governance is crucial in today's digitalized world, as the lines between public and private life are becoming increasingly hazy.

[1] R. Revathi, "Pervasive Technology, Invasive Privacy and Lucrative Piracy- A Critique" 51, JILI 368 (2009)
[2] www.legalservicesindia.com/law/article/10/28/Right-To-privacy
[3] the General Data Protection Regulation (GDPR) 2018.

## Meaning of Privacy

The concept of privacy is not amenable to precise definition. In public law, traditionally privacy means freedom from official intrusion. However, today with the development of science and technology the term privacy has received extended meanings.[4]

**Longman Dictionary** defines privacy as, the state of being away from the presence, notice or activities or others or Secrecy; avoidance of public notice[5].

The **Black's Law Dictionary** defines the right to privacy as, "right to be let alone; the right of a person free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned".

Privacy is the ability of an individual or a group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves.[6] It is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others .Privacy is the voluntary and temporary withdrawl of a person from the general society through physical or psychological means.[7]

According to **Charles Fried**[8], privacy is not simply an absence of information about us in the minds of others; rather is control we have over information about ourselves…The person who enjoys privacy is able to grant or deny access to others. Privacy thus is control over knowledge about oneself.

**Jed Rubenfeld** defines privacy as "the right to make choices and decisions" which forms "the 'Kernel' of autonomy".[9] However going a step further, he introduces the concept of personhood into the doctrine by stating: "some acts, faculties, or qualities are so important to our identity as persons-as human beings-that they must remain inviolable, at least as against the State.

The essence of privacy is no more and certainly no less than the freedom of the individual to pick and choose for himself the time and circumstances under which his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others.

## Data Privacy and Data Protection: Meaning

Data privacy as a notion did not emerge until the late twentieth century, with the introduction of the internet and its rapid usage via computers and mobile phones. Until that time, privacy mostly referred to physical existence and information about an individual, his home, documents, and personal life.

[4] Kiran Deshta, Right to privacy under Indian law 1(Deep and Deep Publication Pvt. Ltd..,New Delhi,2011)

[5] Longman Dictionary of Contemporary English(1986)p.87
[6] Dhruv Jain, The Right To Privacy In India :an overview 90, AIR (June 2009)
[7] DD Basu, "Commentry on the Constitution of India" (vol.3)(2008)
[8] Charles Fried,Privacy,77,YaleLaw journal(1965)
[9] Jed Rubenfeld, "The Right to Privacy",102, Harvard Law Review,p.751 (1989)

Understanding personal data is essential before getting into the concepts of data privacy and protection. This fundamental information paves the way for a more in-depth comprehension of these ideas. Data can be broadly divided into two categories:

- Personal Data: This includes any information that can be used to identify a specific individual, such as their name, address, or other details. Even if you blend multiple bits of data, you can still identify that person. That is why GDPR defines personal data as any information about a live person that may be identified in any manner.
- Non-Personal Data: This refers to information that does not reveal an individual's identify. Even if it is useful, it is not deemed personal data because it does not jeopardize an individual's privacy. Non-personal data includes things like corporate registration numbers, email addresses, and anonymised data.

In the modern digital world, when personal data is a valuable asset that needs to be shielded from exploitation, misuse, and unwanted access, data privacy is a strategic necessity. Having authority over your personal data means determining who can access, distribute, and utilize it. It's important to respect your right to privacy in addition to managing data appropriately. In the technologically advanced world of today, your personal information is like a precious possession that must be shielded from unwanted access.

**Data Protection**

The concept of data protection is closely linked to how personal data is handled, with an emphasis on the fair and legal gathering and use of such data. By ensuring that personal information is handled with care, data protection rules and practices aim to reduce the invasion of privacy. One way to define data protection is as the legal framework that regulates data access and usage in order to prevent misuse of personal information. This area covers both administrative and technical protections, with the latter referring to the legally mandated aspects of data control.

## Constitutional Basis of Privacy in India

Before 2017, the right to privacy was not explicitly recognized as a fundamental right under the Indian Constitution. The jurisprudence on privacy was uncertain, primarily due to conflicting decisions in earlier cases like:

- *M.P. Sharma v. Satish Chandra*[10]: In its Judgment, Supreme Court held that, "a power of search and seizure is, in any system of Jurisprudence, an overriding power of the State for the protection of social

[10] AIR 1954 SC 300

security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of fundamental right to privacy, analogous to the American Fourth Amendment, there is no justification for importing into it, a totally different fundamental right by some process of strained construction."

- *Kharak Singh v. State of UP*:[11] The majority held, Right to Privacy is not guaranteed right under our Constitution and therefore the attempt to ascertain the movements of the individuals which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III. However, Subba Rao J. dissented. This dissenting judgement is a milestone in our privacy jurisprudence. Observing that the right to privacy is an essential ingredient of personal liberty, he held that in a democratic country one cannot lead a peaceful and secured life unless he is assured of freedom from encroachment on his private life. Apart from the physical restraints one is likely to be subjected to, any measure likely to inculcate fear in the mind of a person can also be treated as violation of the right to privacy.

Concerns about privacy have grown in importance over time as a result of government programs like Aadhaar, digital data collecting, and surveillance technologies. The Puttaswamy case, which questioned the legitimacy of data collecting without sufficient protections, resulted from these developments and challenged the Aadhaar scheme

## The Landmark Puttaswamy Judgment

**In** 2009, recognizing the importance of proof of identity and its role in promoting social inclusion, the Indian Government created the Unique Identification Authority of India (UIDAI). The UIDAI was mandated with the task of providing a unique and non duplicable proof of identity to every resident of India. This proof of identity took the form of a unique identification number, that is linked to an individual's iris scans and finger prints as well as basic demographic data. This identification number was given the name 'Aadhaar'. The registration for this card was made mandatory so as to unable the people to file tax returns, opening bank accounts etc.

A retired judge K.S. Puttaswamy, challenged this Aahdaar scheme which the government proposed making mandatory for access to government services and benefits. In **Justice K.S Puttaswamy (Retd.) v. Union of India[12],** the challenge was made before a three- judge bench of the Supreme Court on the basis that the Aadhaar scheme violates right to privacy of the citizens since, the registration of Aadhar is made mandatory. As a result of which all those who don't even want to register themselves, are not left with any option. Moreover, there is lack of data protection laws in India and hence, there are chances that the private information of the people may be leaked if proper care is not taken. This will lead to violation of right to

[11] AIR 1963 SC 1295: (1964)1 SCR 332

[12] (2014) 6 SCC 433

privacy of the individuals. However, the Attorney General argued on behalf of Union of India that the Indian Constitution does not grant specific protection for the right to privacy. He based this on observation made in case of MP Sharma V. Satish Chandra( an eight judge bench) and Kharak Singh v. State of UP( a five Judge bench).

This was in this context, that a Constitutional Bench was set and concluded that there was need for nine judge bench to determine whether there was a fundamental right to privacy within the Constitution.

In a unanimous 9-judge bench decision, the Supreme Court held that **the right to privacy is a fundamental right under Article 21 (Right to Life and Personal Liberty)** and also emanates from Articles 14 (Right to Equality) and 19 (Freedom of Speech and Expression). This judgment not only consolidated the previous developments but also provided a comprehensive framework for protecting privacy rights in the future. The Court recognized privacy as central to human dignity and underpinning values of freedom and liberty. Privacy includes personal intimacies, sanctity of family life, marriage, home, sexual orientation, individual choices, heterogeneity, and the right to be left alone. It facilitates autonomy and guards against excessive State interference. Reasonable restrictions on privacy pass a quadruple proportionality test on - legitimate state aim, rational nexus, necessity, and balancing .

This judgment laid the foundation for all subsequent legal developments related to privacy and data protection in India.

## Legislative Response: The Road to DPDP Act, 2023

In order to design a data protection framework after the Puttaswamy ruling, the government established the Justice Sri krishna Committee. In 2018, the committee put out a draft Personal Data Protection Bill after stressing the importance of a strong data protection law. The bill has had several revisions and introductions over the years. A Joint Parliamentary Committee was tasked with reviewing the 2019 Personal Data Protection Bill after it was criticized. Following multiple discussions and revisions, the Digital Personal Data Protection Act of 2023 was finally passed into law.

Since digital landscapes are changing quickly and personal data is becoming more and more commodified, the efficacy of the legislative attempt to balance the conflicting interests of individual data protection and lawful data processing is called into question by the Digital Personal Data Protection Act of 2023. As it grounds the right to digital data protection in Article 21 of the Constitution and offers a comprehensive and inclusive framework for data handling, the Digital Data Protection Act of 2023 represents a significant milestone in the protection of personal data. This protects citizens from the risks of informational privacy breaches from both public and private entities. [13]

Personal information is valuable. Building business models, understanding clients, running successful marketing efforts, and creating new goods and services are all made feasible by data. However, proper use

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, [2017 (10) SCALE 1]

according to standard guidelines was required, as was the case with many other assets. The Digital Data Protection Act of 2023 aims to restore people's control over their personal data in the wake of the alarming increase in personal data breaches that have revealed millions of people's private information. It also imposes severe penalties on businesses that disregard the law, highlighting the importance of data protection.

**The salient features of the DPDP Act, 2023**

I. **Applicability:** This Act governs India's automated processing of digital personal data, including both offline and online data that has been converted to digital form. If processing operations carried out outside of India are connected to the delivery of products or services inside India, they fall under its purview. According to the Act, "processing" refers to any automated action or series of actions taken on "personal data," such as gathering, storing, using, and exchanging; "personal data" is defined as any information that can be used to identify an individual[14].

II. **Consent:** The existence of a legitimate purpose and the acquisition of the data subject's express consent are the two prerequisites for processing personal data. The foundation of the consent-seeking procedure is the delivery of a notice outlining the types of personal information to be gathered and the reason for processing. It is important to remember that data subjects can withdraw their consent at any time. However, in other situations, such as legitimate use—where a person freely provides data for a specific purpose—or in situations involving government benefits or services, medical emergency, or work relationships, consent is not required. Consent from a parent or legal guardian is required for minors under the age of 18.[15]

III. Rights and duties of data principal: According to the regulations, a data principal—that is, the person whose personal data is being processed—has the following rights: (i) information about how their data is being processed; (ii) the ability to request that their personal data be corrected or erased; (iii) the ability to designate a substitute to exercise their rights in the event of their death or incapacity; and (iv) the ability to seek redress for grievances. Additionally, data principals will have responsibilities, such as (i) not filing baseless or fraudulent complaints and (ii) providing accurate information and not impersonating someone else in specific situations. There is a fine of up to Rs 10,000 for noncompliance with these obligations[16].

IV. Transfer of personal data outside India: The Act permits the transfer of personal data outside of India, with the exception of situations in which the Central Government has announced limitations on transfers to particular nations. This clause gives the Central Government the power to control cross-border data transfers and guarantee that private information is shielded against unsafe or illegal transfers to specific countries.[17]

[14] Section 3, The Digital Personal Data Protection Act,2023
[15] Section 6, The Digital Personal Data Protection Act,2023,
[16] The Digital Personal Data Protection Act,2023, Chapter III, Section 11,12,13,14 and 15.
[17] The Digital Personal Data Protection Act,2023, Chapter IV, Section 16(1).

**V.** Exemptions: According to the Act, under certain conditions, the duties of data fiduciaries and the rights of data principals—aside from data security—will not apply. (i) the prevention and investigation of offenses; and (ii) the enforcement of legal rights or claims are examples of these exclusions. Additionally, the Central Government may, by notification, exempt specific activities from the Act's provisions. In order to balance the rights of individuals and the interests of the group, these exclusions will cover: (i) data processing by government agencies for the objectives of public order and state security; and (ii) processing for statistical, archival, or research reasons[18].

**VI.** Data Protection Board of India: The Act requires the Central Government to establish the Data Protection Board of India, an independent regulatory agency. With duties including monitoring Act compliance, enforcing penalties for infringement, directing data fiduciaries to take corrective action in the event of data breaches, and resolving grievances submitted by aggrieved parties, this Board will be instrumental in monitoring data protection practices.[19]

**VII.** Appeals: Decisions made by the Data Protection Board may be challenged, and the Appellate Tribunal will hear these cases.[20]

**VIII.** Penalties: The severity of the fine varies according to the type and impact of the infraction, as the Act uses a tiered approach to punishments. The Schedule stipulates fines of up to Rs 200 crore for noncompliance with duties pertaining to children's data and up to Rs 250 crore for insufficient security measures that result in data breaches. Following a thorough investigation into the specifics of the infraction, the Data Protection Board of India will decide on the proper punishment.[21]

## Challenges and Criticisms of the Act

Notwithstanding all of these advantages and provisions, the DPDP Act of 2023 has many drawbacks. Critics contend that the Act's effectiveness is diminished and that it may violate fundamental rights due to the extensive exemptions given to the government, especially in the areas of public order and national security. Data security issues and possible inconsistencies with international data protection standards are brought up by the absence of clear requirements pertaining to data localization and cross-border data transfers. The Act's reach and conformity to international best practices are further limited by its silence on important issues like the right to data portability and the right to be forgotten. Concerns concerning the Data Protection Board's independence and impartiality are further raised by the government's influence over its appointment and operations, as well as the concentration of power within the board.

Another major flaw in the Act's framework is the lack of specific rules for automated decision-making and profiling, which are becoming more common in the era of artificial intelligence.

[18] The Digital Personal Data Protection Act,2023, Section 17
[19] The Digital Personal Data Protection Act,2023, Chapter V, Section 18.
[20] The Digital Personal Data Protection Act,2023, Chapter VII, Section 29.
[21] The Digital Personal Data Protection Act,2023, Chapter VIII, Section 33

The Act's eventual success, however, will rely on how well it is implemented, how it is continuously improved, and how steadfastly it is committed to maintaining the values of data protection in the face of changing societal demands and technological breakthroughs. It is just the start of India's journey to guarantee its inhabitants a safe and secure digital future. As a result, the Act is a reflection of the continuous discussion and changing perception of data protection in India, opening the door for a more sophisticated and all-encompassing strategy in the years to come. It represents a dedication, albeit an ongoing effort, to protecting personal privacy in the digital era and promoting an ethical and inventive data economy.

## Conclusion

In India, the right to privacy has undergone a significant and timely transformation, moving from an implicit constitutional value to an openly acknowledged fundamental right. A significant constitutional turning point was reached in 2017 with the landmark Justice K.S. Puttaswamy v. Union of India ruling, which upheld privacy as an essential component of life and liberty under Article 21. Prior to this landmark decision, privacy was unclearly defined, frequently subservient to state objectives, and lacked a clear legal framework, particularly in the digital realm. Following Puttaswamy, privacy gained both moral and legal standing, necessitating more robust frameworks to protect personal freedom, dignity, and privacy of information.

At the end of this voyage, the Digital Personal Data Protection (DPDP) Act, 2023, was passed, operationalizing the right to privacy in India's digital environment. The Act reflects a rights-based approach to data protection by including concepts such as purpose limitation, data minimization, informed consent, and accountability procedures. A Data Protection Board is also established to guarantee adherence and settle disagreements.

The Puttaswamy ruling and the DPDP Act taken together demonstrate India's increasing dedication to upholding individual liberties in the information era. They emphasize how important it is to strike a balance between personal liberty, governance, and technical progress. This legal path confirms that privacy in India is no longer a passive right but rather an active, protected right that is resistant to both private and state intrusions in the digital age, even though implementation and enforcement are still the next important steps.