

K.S. Puttaswamy v. Union of India to Data Protection: The Evolution of Privacy Jurisprudence in India

^{1st}Dr Pamarthi Satyanarayana, ^{2nd}Dr S. Udayakumar, ^{3rd}P Sowjanya,

¹Assistant Professor, School of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai.

²Assistant Professor, School of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai.

³Research Scholar, Dept of Law, Sri Padmavati Mahila Visvavidyalayam (Women's University), Tirupati, Andhra Pradesh, India.

Abstract: Historically, the development of privacy jurisprudence in India is among the key changes in constitutional and legal thinking, especially in reaction to the fast technological changes and the expansion of the digital economy. The historic ruling in the case of K.S. Puttaswamy v. Union of India was a change of direction since it unambiguously acknowledged the right to privacy as a primary right under Article 21 of the Constitution. This ruling did not only redefine the boundaries of individual freedom, but also developed a strong doctrine of dignity, autonomy and informational self-determination. Based on this constitutional basis, India has been making great legislative strides to control data protection, and the Digital Personal Data Protection Act, 2023 has been introduced. This paper takes a critical look at how privacy jurisprudence has taken the shape of fragmented judicial acknowledgment in pre-Puttaswamy cases up to consolidation in modern legal approaches. It examines the interaction of constitutional values and statutory regulation, including the aspect of consent, data handling, government surveillance, and responsibility of commercial actors. The paper also examines the implementation problems such as regulatory lapses, limitations to enforcement and the changing role of technology. The paper has illuminated the necessity of coherent and future oriented privacy regime by taking a doctrinal and analytical approach. It concludes that even though India has come a long way, legal innovation and institutional fortification is needed to guarantee effective privacy protection in the digital era.

Keywords: Privacy Jurisprudence, Fundamental Rights, Data Protection Law, Informational Privacy, Indian Constitution Law.

1. Introduction

The establishment of privacy as a legal right in India has been a slow and a constantly developing process that has been informed by judicial interpretation, constitutional philosophy and socio-technological developments. The right to privacy is not explicitly listed in the Constitution of India as a fundamental right unlike a number of other constitutions of modern times. But the extensive and evolving interpretation of Part III of the Constitution, and Article 21, in particular, the right to life and the liberty of the person, has allowed the judiciary to broaden its domain to embrace privacy as inherent in human dignity and autonomy. This development indicates the flexibility of the principles of the constitution in responding to modern problems.

During the early years of constitutional adjudication, the Indian judicial system took a comparatively restrained viewpoint of personal liberty and frequently restricted it to physical confinements. However, as time passed the Supreme Court adopted a broader purposive interpretation, in which it realized that the right to life was more than existence. It consists of the right to a dignified life, the right to make individual decisions, and being independent about one's body and personal data. In the context of this, privacy became a precondition to the substantive realization of fundamental rights.

Global legal changes and comparative constitutional jurisprudence have played a significant role in creating privacy as a legal right. Privacy has been established as a basic human right in international human rights documents like Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. These principles have commonly been utilized by Indian courts to interpret the constitutional clauses so as to align with the international norms, thus strengthening the normative foundation of privacy.

The accelerated development of technology and internet communication has additionally enhanced the urgency of acknowledging privacy as a unique legal right. The spread of the internet, mobile phones, and services that are based on data has revolutionized how personal information is created, stored and shared. In this online world, people are more susceptible to misuse of data, surveillance, and unauthorized access to personal information. Such developments have pointed at the inefficiency of the traditional legal frameworks and emphasized the need of a strong privacy regime.

2. Pre-Puttaswamy Jurisprudence: Disjointed Awareness of Privacy

Before the landmark decision in *K.S. Puttaswamy v. Union of India*, the awareness of the right to privacy in Indian constitutional law was patchy. The judiciary found itself in a dilemma on whether or not privacy could be regarded as a fundamental right, and in many cases gave contradictory decisions which also indicated a lack of doctrinal clarity. This era of jurisprudence is defined by gradual acceptance of privacy in particular situations as opposed to its wholesale acceptance as a right.

Pre-Puttaswamy Jurisprudence: Fragmented Recognition of Privacy

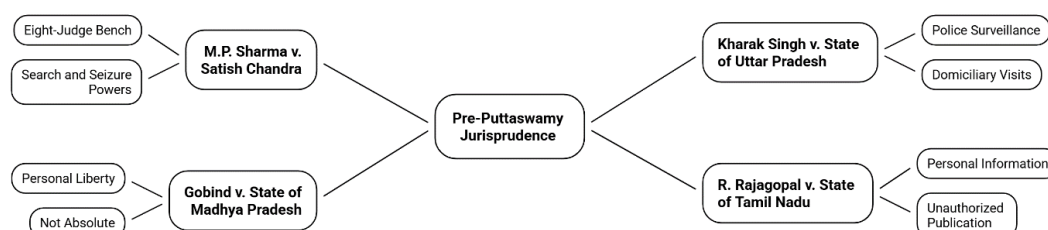


Fig: Pre-Puttaswamy Jurisprudence: Fragmented Recognition of Privacy

M.P. Sharma v. Satish Chandra was one of the first cases to deal with the issue of privacy: an eight-judge panel of the Supreme Court ruled that the Constitution did not explicitly grant a right to privacy. The case was presented under the situation of the search and seizure powers and the Court dismissed the argument that the power violated one of the fundamental rights to privacy. In a similar case, *Kharak Singh v. State of Uttar Pradesh*, the Court considered the police surveillance measures, such as domiciliary visits. Although most of them rejected that there was a general right to privacy, it acknowledged that Article 21 which guaranteed personal liberty could be infringed upon by means of unauthorized entry to the home of a person. It is worth noting that the minority opinion in *Kharak Singh* provided the basis of acknowledging privacy as a fundamental right in the future.

In spite of these initial restrictions, later case law started to broaden the definition of privacy in particular situations. In *Gobind v. State of Madhya Pradesh*, the Supreme Court recognised that privacy was deductible through the right to personal liberty, though it did not go a notch higher to declare it as an absolute right. In the same case, *R. Rajagopal v. State of Tamil Nadu*, the Court acknowledged the right to privacy, as far as the right to protection against the unauthorized publication of personal information is concerned. These rulings showed a slow transition into acknowledging privacy, although in a bit-by-bit fashion.



The lack of a coherent doctrinal framework can also be considered the reason why the pre-Puttaswamy jurisprudence was so fragmented. The courts tended to base their arguments on case-by-case logic, and they did not state a single theory of privacy. This caused confusion over the extent and scope of the right, especially in new frontiers like informational privacy and data protection. Moreover, the incredibly fast development of technology revealed the weaknesses of the current legal principles which were not aimed at dealing with the challenges of the digital era.

The other major problem at this time was the indecisiveness concerning the connection between privacy and other basic rights. Some of these judgments associated privacy with individual freedom, whereas others considered it as freedom of expression or dignity. This lack of consistency made it impossible to develop a consistent jurisprudence and provided people with no definite grounds to make claims about their right to privacy.

3. The Puttaswamy Judgment: A Transformative Impact

The case of K.S. Puttaswamy v. Union of India is considered the turning point in the development of the Indian privacy jurisprudence. The ruling, issued by a unanimous nine judge Supreme Court, is definitive that the right to privacy is an essential right that is safeguarded in Part III of the Constitution. By so doing, the Court reversed previous cases like M.P. Sharma and Kharak Singh to the degree that they had rejected the existence of such a right, clearing up decades of doctrinal confusion.

The Puttaswamy case is not only notable in acknowledging privacy but it also describes the concept in detail. The Court recognized privacy as a complex right including bodily integrity, informational self-determination, and decisional autonomy. This broad interpretation indicates how the Court has recognized the various aspects in which privacy may be impacted in the contemporary society especially due to technological innovations and online communication.

One of the most important contributions of the judgment consists in the creation of a strong model of the evaluation of limitations on privacy. The Court provided a triple test that any invasion of privacy should prove the legality, necessity and proportionality. This system guarantees that the state activity is controlled by strict control and that the rights of persons are not arbitrarily limited. It has since formed a foundation of constitutional adjudication in cases of privacy and other rights that are related to it.

Another point that was highlighted in the judgment was the inherent connection between privacy and human dignity. The Court emphasized that the notion of privacy is a crucial part of individual personality growth and independence, indicating that it strengthened its status as a key principle in the Constitution. This view makes the Indian jurisprudence consistent with international human rights norms and highlights the necessity to defend individual rights in a democratic society.

Moreover, the Puttaswamy ruling has impacted extensively on policy and legislative advancements. It provided the basis of developing overall data protection legislation and emphasized the necessity to have regulatory tools to regulate the gathering and handling of personal information. The ruling recognized the problems of the digital age, such as data surveillance, profiling, and the involvement of private actors in the processing of personal data.

4. Based on Constitutional Right to Statutory Framework: Data Protection Laws in India

The establishment of privacy as a right in K.S. Puttaswamy v. Union of India established a landmark in the Indian jurisprudence and a statutory framework was to be developed to govern data protection. Although the ruling established the constitutional basis, it also underscored the pressing necessity of legislative intervention to put into practice informational privacy in an ever more digitalized society. Before this development, the law of data protection in India was predominately regulated by the Information Technology Act, 2000, and the related



regulations on sensitive personal data. Nevertheless, these specifications were sector-specific and narrow in scope, and could not effectively cover the intricacies of current data processing practices.

To comply with this court order, India has engaged in a series of legislative efforts to create a sound data protection framework. Such initiatives led to the adoption of the Digital Personal Data Protection Act, 2023, which is one of the first steps towards the codification of privacy rights. The Act presents a well-organized framework grounded on internationally accepted principles like consent, purpose limitation, data minimization, and accountability. It establishes major participants, such as data principals and data fiduciaries, thus making clear the rights and duties of the individuals and entities participating in data processing.

The focus on consent as the main lawful data processing is one of the highlights of the Act. The consent should be free, informed, specific and unambiguous as it should be consistent with the constitutional demand of autonomy and control over personal information. Other rights offered by the Act include the right to access their data, right to correct inaccuracies and right to withdraw their consent. These rights seek to empower the users and promote transparency in data handling practices.

The Act provides an institutional mechanism of enforcement and resolution of disputes through the establishment of the Data Protection Board. The Board has the responsibility of overseeing compliance, investigating violations and penalizing where appropriate. Also, the Act requires the notification of data breaches and the creation of reasonable security safeguards by entities, enhancing accountability.

Even in the face of these developments, there still are some concerns. The Act gives state agencies very generous exemptions like national security and public order, and the question is whether it can be abused and not regulated. Moreover, the problems of cross-border data flows, independence in regulation, and enforcement still remain a challenge. Another argument by critics is that the consent-based model might not be able to capture the complexities of the data-driven technologies where users do not have meaningful choice.

Simply put, the shift towards constitutional protection to statutory restriction is a significant stage in the development of the Indian privacy jurisprudence. Although the Digital Personal Data Protection Act, 2023 is a positive step, its success will be determined by its implementation, institutional capacity, and the capacity to adjust to the new technological realities.

5. Current Issues: Surveillance, Technology and Gaps in Enforcement

The high rate of development of digital technologies has brought new and complicated problems in terms of privacy protection in India. Among them, the growth of surveillance systems, whether the state or the private organizations, is a serious challenge to the independence of individuals and civil rights. Facial recognition and biometric data, artificial intelligence-based analytics, and other surveillance technologies allow monitoring people around-the-clock, without their own awareness or permission. Although these actions can often be defended as being based on national security and public safety, they pose significant questions about proportionality, necessity and culpability in a constitutional system.

The guidelines established in *K.S. Puttaswamy v. Union of India* state that any violation of privacy should be justified by the law, have a legitimate purpose, and be reasonable to the purpose being fulfilled. But the lack of a complete surveillance law in India leaves a vacuum in its regulation, and there is the possibility of power abuse. Current systems of interception and surveillance are not transparent and are not subject to external control, which makes the role of arbitrary state actions more dangerous.

The privacy situation is also complicated by technological advancements. With the emergence of big data analytics, machine learning, and algorithmic decision-making, the ability to collect and process large volumes of personal information has become feasible. These technologies are frequently opaque, so that people cannot easily



see how their data is being utilized, or appeal against decisions taken about them. Algorithms bias, profiling, and automated decision-making are some of the issues that challenge the fairness, discrimination, and accountability.

The other significant issue is the gaps in enforcement of the current legal system. The Digital Personal Data Protection Act, 2023 is a more detailed framework on how data protection should be achieved, but its implementation must be effective in order to succeed. Formation of regulatory authorities, resource distribution and creation of technical skills are important elements in making sure that compliance is achieved. In practice, the enforcement can be delayed, unawareness and institutional capacity can prevent the implementation of privacy rights.

The involvement of the non-governmental actors, especially the social media and technology corporations, is also a challenge. These organizations manage large digital ecosystems and have a major impact on the flows of data and user activity. Their own business models are usually based on data monetization and this results in conflicts of interest between business and privacy. To ensure accountability of such entities, it is important to have not just legal regulation but also ethical governance and self-regulatory mechanisms.

Moreover, the data transfers across the borders make enforcement activities more complicated, as data is often stored and processed across several jurisdictions. This undermines the question of jurisdiction, data sovereignty, and international collaboration. The absence of transparent and coherent regulatory frameworks could make it hard to take legal action against the privacy breach.

6. Conclusion and Future of privacy jurisprudence in India

The evolution of privacy jurisprudence in India reflects a dynamic interplay between constitutional principles, judicial innovation, and legislative development. Privacy is a basic right as understood in *K.S. Puttaswamy v. Union of India* which offers a solid normative base and has changed the perception of the rights of the individual in the digital era. The given constitutional breakthrough has been supported by the legislative improvements, in particular, the introduction of the Digital Personal Data Protection Act, 2023, which aims to conceptualize informational privacy via a formal legal framework.

Nevertheless, the road to efficient privacy protection is not over yet. New issues like surveillance, algorithmic governance and cross-border data flows still challenge the strength of the legal mechanisms in place. The disjuncture between law and its application is still a pressing issue, and the necessity of better institutional ability and regulation.

In the future, future of privacy jurisprudence in India will be pegged on its capacity to change with the changing rapid technological and societal contexts. It is necessary to have ongoing judicial involvement in expounding and refining privacy principles and legislative responsiveness to new risks. Enhancing user empowerment, accountability, and transparency should continue to play a pivotal role in this process.

Finally, protecting privacy is a complex issue that needs a cooperative approach between the state, the private sector, and the civil society. Through creating a balanced solution that would combine innovations and safeguarding of rights, India will be able to create a strong and visionary privacy regime that would support constitutional principles and respond to the digital age challenges.

References

- [1] Ansari, M. B., & Haque, I. (2024). Privacy Rights and Social Media. *International Journal for Research in Applied Science and Engineering Technology*. <https://doi.org/10.22214/ijraset.2024.58023>
- [2] Ardhapurkar, S. B., Srivastava, T., Sharma, S., Chaurasiya, V. K., & Vaish, A. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. *International Journal of Engineering Science and Technology*, 2(5), 942–951.

- [3] Basu, S. (2012). Privacy Protection: A Tale of Two Cultures. *Masaryk University Journal of Law and Technology*, 6(1), 1–34. <https://journals.muni.cz/mujlt/article/download/2593/2157>
- [4] Bhandari, V., & Sane, R. (2018). Protecting Citizens From the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251982
- [5] Grover, D. J., & Singh, R. (2024). The law of right to privacy in india: protecting privacy in the digital era: challenges. *ShodhKosh Journal of Visual and Performing Arts*, 5(1). <https://doi.org/10.29121/shodhkosh.v5.i1.2024.3498>
- [6] Jindal, T. (2024). Right to Privacy as a Fundamental Right in India: Evolution, Challenges, and the Impact of Digitalization. *International Journal For Multidisciplinary Research*, 6(6). <https://doi.org/10.36948/ijfmr.2024.v06i06.31832>
- [7] Kumaraguru, P., & Sachdeva, N. (2012). Privacy in India: Attitudes and Awareness V 2.0. *Social Science Research Network*. <https://doi.org/10.2139/SSRN.2188749>
- [8] Mittal, S., & Sharma, P. (2017). *A Study of the Privacy Attitudes of the Users of the Social Network(ing) Sites and Their Expectations from the Law in India* (pp. 1038–1051). Springer, Cham. https://doi.org/10.1007/978-3-319-76348-4_100
- [9] Prashanth, S. K., & Devaiah, N. G. (2024). *Privacy on New Media Platforms*. <https://doi.org/10.20944/preprints202405.0497.v1>
- [10] Satapathy, A. (2024). *The use of social media as evidence according to indian law*. <https://doi.org/10.5281/zenodo.11115757>
- [11] Siwal, A. (2021). *Social Media Platform Regulation in India – A Special Reference to The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (pp. 215–232). Nomos Verlagsgesellschaft mbH & Co. KG. <https://doi.org/10.5771/9783748929789-215>
- [12] Tiwari, S. K., & Mishra, K. G. (2024). A case study on right to privacy. *ShodhKosh Journal of Visual and Performing Arts*, 5(5). <https://doi.org/10.29121/shodhkosh.v5.i5.2024.2967>
- [13] Uppaluri, U., & Shivanagowda, V. (2015). Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2660569