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

THE EVOLVING ROLE OF THE SUPREME COURT OF INDIA AS A WATCHDOG OF DIGITAL PRIVACY: A DOCTRINAL AND POLICY REVIEW

Palak Anand

ABSTRACT

Technological innovations have grown significantly in the short term changing the relationships between the State and individuals, the topic of privacy, surveillance, and the web of digital governance is becoming more and more controversial. In India, the issues gained constitutional importance when the Supreme Court gave the concept of right to privacy a constitutional status as a fundamental right in Article 21 of the Constitution in Justice K.S. Puttaswamy (Retd.). v. Union of India. The ruling was a monumental change in the Indian constitutional jurisprudence and made the autonomy of individuals, their dignity, and self-determination of information the key driver in the discussion of digital governance. The research paper is a policy and doctrinal study of how the Supreme Court of India has changed to become the champion and protector of digital privacy. It looks at the impacts of judicial interpretations on the privacy jurisprudence in relation to Aadhaar frameworks, state surveillance systems, and data governance systems as well as the growing use of governance technologies. The paper is a critical analysis of how the Court exercised proportionality and constitutional scrutiny in order to weigh the technological efficiency and national interests against the fundamental rights.

Moreover, the paper examines the Supreme Court involvement of legislative events, especially the Digital Personal Data Protection Act, 2023. It evaluates whether judicial review has been sufficient to respond to the concerns of citizens with regard to the protection of information, informational autonomy as well as executive discretion without necessarily frustrating the ability of the State to govern effectively. This paper suggests that the Supreme Court has been

central in bringing the issue of digital privacy to the constitutional status. It however argues that sustained court watchfulness and a refinement of its doctrine is imperative to accommodate changing surveillance habits and new challenges to the Indian data-driven governance environment.

Keywords: Digital Privacy, Surveillance, Data Protection, The Supreme Court of India.

INTRODUCTION

The speed at which digital technology is being adopted has completely altered the way governments are conducted and how they interact with people. There is massive personal data gathering, storage, processing and analysis in digital form than ever before in the State sector or the private sector. In India, Digital India programme, growth of e-government systems, the Aadhaar identification system, and so forth, represent a concerted step towards the digitisation of the country to enhance the efficiency of the administration, its transparency, and delivery of services to the population.[1] Even though these technological projects have immense developmental and governance advantages, there are deep concerns that relate to mass surveillance, profiling, diminution of individual agency, and civic privacy risks.

These issues have been compounded by the lack of an elaborate and effective legal system that regulates the protection of personal data in India over an extended period of time. The absence of explicit statutory protections is what made a regulatory vacuum, allowing the unchecked data collection and processing by the state governments and individuals. This atmosphere increased the danger of unreasonable surveillance and abuse of personal data, which weakened the individual rights in a fast digitalising society. The Supreme Court of India has become an important institution in protecting digital privacy in an effort to fill this constitutional and regulatory vacuum.

The landmark decision of the Supreme Court in Justice K.S. Puttaswamy (Retd.).- The Union of India This decision was a landmark in the Indian constitutional jurisprudence tradition. The Supreme Court held that the right of privacy is one of the significant constituents of the Constitution of India under Article 21 of the Indian Constitution, thereby locating the right of privacy under the constitutional principles of dignity, autonomy, and informational self-determination.[2] Such control of people over collecting, using, and distributing their personal

[1] NITI Aayog, *Strategy for New India @75* (2018).
[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

information was affirmed in the judgment which contrasted with the historical view of privacy as a marginal or subservient constitutional value. This change of doctrine raised privacy up to the forefront of the Indian list of fundamental rights.

The period after Puttaswamy has engaged the Supreme Court with more complex issues that arise out of digital governance. The matter of biometric identification systems, electronic surveillance systems, internet blockages, and data control systems has later been echoed in judicial debate. Using proportionality and rights-based analysis, the Court has tried to weigh and balance competing state interests between national security, order in the United States, and technological innovation on the one hand, with the rights and freedoms of people in the Constitution on the other. This shows the engagement of the Court in more critical matters, thus underlining the Court as an evolving force, a constitutional watchdog in the online world.[3]

The paper is intended to investigate the role which the Supreme Court plays in shaping the development of cyberspace privacy and protection in India. The work will investigate the conceptual foundations which have been laid down in this respect, as far as the role of the Court in new governance technologies is concerned, whether the judiciary watchfulness is consistent in this respect to an appropriate degree in order to cope effectively with this emerging cyberspace threat. Finally, this study will explore whether this system is efficient in ensuring that cyberspace change in India takes place in an appropriate constitutional framework.

DOCTRINAL EVOLUTION OF PRIVACY JURISPRUDENCE IN INDIA (PRE- AND POST-PUTTASWAMY)

A. Pre-Puttaswamy Jurisprudence: Fragmented Recognition

Right to privacy in India was not recognized in the Constitution and developed in an unstructured fashion through the thinking of the courts. In the case of M.P. Sharma v. Satish Chandra, an 8 Judge Bench of the Supreme Court of India, though, unlike the United States, the Constitution of India was not such an amendment, and therefore there was no such thing as a right to privacy of a Constitution.[4]

This position was, again, reiterated in the case of Kharak Singh v. State of Uttar Pradesh, in which the majority dismissed the claim of privacy as a fundamental right. However, in the case of Kharak Singh, there was a minority judgment by Justice Subba Rao, who recognized privacy

[3] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
[4] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).

as a facet of personal liberty, an intrinsic right in the Constitution, in Article 21.[5] Even though the Supreme Court lost in the majority of these case laws in the first instances, the Supreme Court did, in fact, recognize privacy interests, to an extent, in certain situations and contexts. In the case of Gobind v State of Madhya Pradesh, privacy was recognized as a fundamental right flowing from Article 21 but in a rejecable and importable manner.[6]

Consequently, in future decisions there was a reasonable balance of the right to privacy in the situations of telephone tapping, personal choices, and sexual autonomy, etc.[7] However, the presence of a clear doctrinal foundation led to unstructured application of laws and unpredictability regarding the number of rights a person could claim with respect to privacy.

B. Post-Puttaswamy ‘s Jurisprudence. Consolidation of the Constitution

The K.S. Puttaswamy (Retd) v. Union of India case is the first case where the apex court recognized the right to privacy as a fundamental right, and this marked the beginning of Puttaswamy’s privacy doctrine, where the court linked privacy to fundamental rights enshrined in the Constitution, especially Articles 14, 19, 21,[8] and there was also another fundamental right drawn, being the first and vital step to the case of M.P. Sharma and Kharak Singh. The Right to Privacy has its origin in Human Dignity, Autonomy, and Self-Determination. In this case, Puttaswamy constructed the first and the most elaborate form of the Right to Privacy and on which he has, and will be, in the future, acting as a part of the Right to Privacy. Puttaswamy is also the first case to introduce the principle of proportionality and the normative requirements that the state must fulfil, which are the aspects of fairness, legitimation, and the purpose of the state. This framework has since informed a number of the state of the right to privacy in the digital age, and these cases include Surveillance and Internet Restrictions, to cite a few, apart from Aadhaar. The post Puttaswamy era has also witnessed the apex court and also the privacy jurisprudence matured, as post Puttaswamy has witnessed the apex court and also privacy jurisprudence matured as post Puttaswamy has witnessed not only the privacy and for the first time in the history of India and the digital realm ‘Right’ matured.

[5] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).
[6] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India)
[7] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India); *People’s Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).
[8] Ibid (2)

JUDICIAL SCRUTINY OF AADHAAR, SURVEILLANCE, AND DIGITAL GOVERNANCE

After Puttaswamy, the Supreme Court of India began scrutinizing the digitization of governance, focusing in particular on the clearance of biometric data in relation to state surveillance. Puttaswamy's Post-Privacy doctrine most applications reside with Justice K. S. Puttaswamy (Aadhaar-5J) v. Union of India, where the constitutional validity of the Aadhaar programme is not without question.[9] The CC's justification for using Aadhaar in the welfare delivery, taxation, and in the financial regulatory framework was struck down in the CC's observations as unreasonable intrusion of one's informational privacy of the provisions that allowed the private sector not to render services unless users authenticated themselves through Aadhaar.[10] Through this ruling, the Court showed that it was ready to take on the challenges that the technology-linked to Aadhaar issued by conducting a proportionality analysis. The Supreme Court also willingly considers the state surveillance systems. In Puttaswamy in People's Union for Civil Liberties v. Union of India, the Court, before Puttaswamy, issued a set of instructions, which, in the form of guidelines, were to operate as procedural limitations of the power to telephone-tap as arbitrary power.[11] The right to privacy has legal implications in terms of political existence and its application in Puttaswamy, which these safeguards gained to a greater degree of constitutional depth as surveillance was considered a serious violation of constitutional political rights.' Nevertheless, it has been argued that the Court has been too tentative, and in fact too mute, in taking on the legitimacy of the surveillance of the modern state, such as the Telecom Act, and the Information Technology Act, 2000. With respect to Digital Governance, the closure of the internet, and the control of data, the Courts have also experienced the restraints of such governance. The Court has, in Anuradha Bhasin v Union of India, recognized that the right to access the internet is part of the right to freedom of expression[12]. The proportionality principle and periodicity of review were also discussed in relation to the closure orders. While the court did not expressly say that internet access is a fundamental right, the judgment did bolster judicial scrutiny on the executive branch's encroachments within the digital space. Those judgements are a clear manifestation of the Supreme Court playing 'watchdog' role within the digital space and exercising its supervisory

[9] *Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (India).
[10] Apar Gupta, *Surveillance and the Indian Constitution*, 12 NUJS L. Rev. 45 (2019).
[11] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).
[12] Ibid (3)

authority to ensure that digital governance not be exercised to the detriment of constitutional rights.

THE SUPREME COURT AND THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 - Named as the DPDP Act, it was an initial move at the comprehensive level of regulation of personal data collection, processing, and storage in the digital age. The passing of the Act has more to do with the legislative reaction to the constitutional dicta of the Supreme Court as founded in Justice K.S. Puttaswamy (Retd.),. v. Union of India, which acknowledged the right to privacy as one of the fundamental rights in Article 21 of the Constitution.[13] Although the main issue of legislation is the DPDP Act, the burden of the digital privacy watchdog still lies with the Supreme Court that still plays a leading role in interpreting and future usage of the DPDP Act.

DPDP Act is contrived conceptually on the grounds which are described in the Puttaswamy, especially the consent-based data processing, the limitation of the purpose and the proportionality. These principles aim at enforcing that individual data should be gathered and processed in a way that preserves their autonomy and informational self determination.[14] Nonetheless, with all the progressive purposes, the Act has received extensive criticism because of granting the executive vast and mostly unaggregated discretionary authorities. It is worth mentioning that such provisions that provide exemptions to the State based on such grounds as the sovereignty, the public order, or the national security pose significant constitutional problems, as they may lead to uncontrolled surveillance and excessive processing of the data provided by the state authorities without serious constraints.

These issues are further complicated by the fact that the DPDP Act lacks clear mechanisms of judicial oversight. The Act fails to incorporate institutional checks and balances, thus giving rise to a regulatory system in which an executive action can be effectively seen as accountable. This institutional weakness puts more onus on constitutional courts, to act post facto, as opposed to protecting rights by providing in-built statutory checks. The way the Supreme Court would interact with the DPDP framework is of vital importance in this regard. Judicial review will play a crucial role to make sure that the delegated legislations, executive notifications and

[13] Supra (2)
[14] Digital Personal Data Protection Act, No. 22 of 2023, §§ 7, 17 (India).

enforcement measures under the DPDP Act are constitutional and do not exceed the proportionality framework under the right to privacy.[15]

Although the DPDP Act represents such an important step in the beginning stages of the establishment of data protection in India, the constitutional validity of the DPDP Act would be proved finally through a long process of judicial scrutiny. As the guardian of the Constitution itself, the SCC must not only protect the DPDP Act from any judicial challenges raised by citizens but also ensure through its jurisprudence that the tools of such governance under the statute would not in any manner reduce the basic right of privacy in the Indian constitutional scheme.

POLICY GAPS, INSTITUTIONAL LIMITATIONS, AND THE NEED FOR JUDICIAL VIGILANCE

Although the development of online privacy into becoming an existing right in the constitution helped through the intervention of the Supreme Court in India, some of the important policy deficiencies in this area continue to exist in the case of India's data governance framework. Even though it was Justice K.S. Puttaswamy (Retd.) who declared in R., v. The privacy as one of the fundamental rights in Union of India who's appropriate enforcement is contingent upon their robust legal framework as well as an independent institution to guarantee respect for data protection norms.[16] Recognition in the constitution alone does not serve the purpose without the regulatory frameworks that would make possible the ideals of the law in the protection of the individual.

In this regard, the Digital Personal Data Protection Act of 2023 takes a clear progressive stance in the legal sphere, as it confirms the rights and responsibility to protect personal data. Nevertheless, some concern still remains with regards to the independence of the concerned regulatory body established under the act[17]. There can be no doubt that the lack of complete independence of the executive authority casts a dark cloud on the objectivity and efficiency of the enforcement procedures. Such weakness of the structure poses a threat to the loss of confidence to the regulatory system by the population and over-imposes a skewed responsibility over judicial review to correct infringements on privacy rights. This can lead to the situation where courts have no choice but to become the main corrective intervention, as

[15] Gautam Bhatia, *The Transformative Constitution* 287–89 (2019).
[16] Digital Personal Data Protection Act, No. 22 of 2023, § 19 (India).
[17] Bimal N. Patel et al., *Indian Constitutional Law* 421–23 (2018).

opposed to being a control agent who looks over the functioning of well-performing regulatory processes.

Moreover, the courts themselves are structurally and institutionally constrained to address the threat of technology that changes at rather high rates. The judiciary involvement in the area of digital privacy is in most cases reactive as courts only come in after they have violated the constitution. This reactive stance constrains the judiciary in predicting future harms that would emerge as a result of the development of surveillance technologies, artificial intelligence, and data analytics. Moreover, digital systems also require technical expertise that is specialist in nature, something that the ordinary adjudicatory procedures might not possess. The lack of sufficient judicial capacity-building and availability of specialised help also limits proper management in the technologically intensive cases.[18]

The other area that is of critical gap is the lack of development in the articulation of informational privacy in relation to data processing by the private sector. Although the primary role of the Supreme Court has been to challenge the state action, in increasing numbers, the quasi-sovereign power of private corporations over personal information is introduced by massive data gathering, profiling, and algorithmic decision-making. Without well defined standards of judicial review of the horizontal use of privacy rights, individuals will still be susceptible to non-state level harms of digital nature, such as data misuse, behavioural manipulation and discrimination. Such inadequacies highlight why there is a great need of judicial vigilance that is sustained. The Supreme Court still needs to strengthen the proportionality criteria, demand transparency and accountability in executive decision-making, and make sure that digital governance systems are changed according to the constitutional principles. It is only through its active and foresighted monitoring that the Court can adequately carry out its mandate of becoming an effective watchdog on digital privacy in an ever more data-intensive society.

CONCLUSION

Supreme Court of India's influence is definite as well as dynamic in molding the constitution of digital privacy. The jurisprudence of privacy has shifted from judicial diachronicity to a constitutional norm of dignity, autonomy, and self-determination of information. The case of Justice K.S. Puttaswamy (Retd.) & Ors. v. Union of India is a landmark case that, apart from

[18] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

the task of constitutionally embedding privacy in the Indian Constitution, also established the Court's primary regulatory oversight of the Indian digital order. The subsequent judicial engagement of Aadhaar, surveillance, and internet freedom is indeed cautious, but in no way minor, exercise of claim dominance over constitutional regulation. The Court has sought to sound a note of caution, through the doctrine of proportionality, on the possible reconciliation of technology, the state, and the citizens. The gravity of the matter has also been far from ideal. The recently enacted legislation, the Digital Personal Data Protection Act 2023, though a positive development institutionally, has also, as a consequence, stressed the lack of independence, discretion, and accountability that the Court possesses. These concerns shall solidify the future role of the judiciary in fulfilling the constitutional mandate that legislative enactments shall not, in any case, violate the fundamental rights of the people.[19]

The same time, would like to note that during the technology and reactive adjudication, the Supreme Court's oversight role is conditioned by the technology's complexity and the reactive adjudication frame. With the digital ecosystem and data capture by non-state actors, the Supreme Court is called to deepen the ‘horizontal application’ of the principles of privacy and non-state injury. Finally, the digital privacy legislation in India needs to be more than a legislative shield. It needs ‘judicial autonomy’ and ‘dogmatic clarity’ as well as ‘constitutional courage’. The Supreme Court of India, in addressing the challenges of the ‘data-driven era’, needs to meet the technology head-on and ‘engage’ it within the ‘constitutional mandate’ to bolster the’ foundational values’ of democracy in the Republic of India.

REFERENCES

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
2. *Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (India).
3. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
4. *People’s Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).
5. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
6. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).
7. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).
8. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India).
9. Digital Personal Data Protection Act, No. 22 of 2023 (India).
10. NITI Aayog, *Strategy for New India @75* (2018).

[19] Digital Personal Data Protection Act, No. 22 of 2023 (India).

11. Apar Gupta, *Surveillance and the Indian Constitution*, 12 NUJS L. Rev. 45 (2019).
12. Gautam Bhatia, *The Transformative Constitution* 287–89 (2019).
13. Bimal N. Patel et al., *Indian Constitutional Law* 421–23 (2018).
14. Rishabh Dara, *AI and Legal Research Trends in India*, 18 Indian J. L. & Tech. 44 (2023).
15. Ministry of Electronics & Information Technology, *SUVAS Launch Note* (2023).
16. Supreme Court of India, *SUPACE Launch Note* (2021).
17. National Judicial Data Grid, *Pendency Statistics* (2024).
18. e-Courts Mission Mode Project, *Phase III – Vision Document* (2023).