
JUDICIAL ACTIVISM IN THE DIGITAL AGE: THE ROLE OF INDIAN COURTS IN FILLING LEGISLATIVE LACUNAE OF DATA PRIVACY

Savita S Pattanshetti, Research Scholar, Department of Law, Mansarovar Global University, Sehore, Madhya Pradesh

Tai Chourashiya, Associate Professor, Dean, Faculty of Law, Mansarovar Global University, Sehore, Madhya Pradesh

ABSTRACT

The rapid expanding of digital technologies has transformed governance, commerce, and social interactions, resulting in unprecedented 'collection and processing of personal data'. In India, the absence of a comprehensive data protection framework for several decades created significant legislative gaps that exposed citizens to privacy risks arising from state surveillance, biometric identification systems, and digital platform governance. This paper examines the role of judicial activism in addressing these legislative lacunae and shaping the constitutional foundations of data privacy protection in India. Through a doctrinal and analytical examination of landmark decisions, including '*M.P. Sharma v. Satish Chandra*, '*Kharak Singh v. State of Uttar Pradesh*, '*Gobind v. State of Madhya Pradesh*, '*R. Rajagopal v. State of Tamil Nadu*, '*PUCL v. Union of India*, and '*Justice K.S. Puttaswamy v. Union of India*', the study traces the evolution of privacy from an implied 'constitutional value to a fundamental right under Article 21'. It further analyses how judicial intervention influenced legislative developments culminating in the 'Digital Personal Data Protection Act, 2023'. The paper argues that Indian courts acted as de facto data protection regulators by establishing principles of informational privacy, proportionality, dignity, autonomy, and accountability before statutory regulation emerged. It concludes that despite the enactment of the DPDP Act, continued judicial oversight remains essential to ensure rights-centric digital governance and constitutional protection in an increasingly data-driven society.

Keywords: Judicial Activism; Data Privacy; Informational Privacy; Digital Personal Data Protection Act, 2023; Digital Constitutionalism.

Introduction

In the twenty-first century, the nature of governance has dramatically changed because of the introduction of technology into all types of public administration and private life. Today, ‘most valuable asset is information in the current economy’; some call it the “new oil” because of its incredible commercial and strategic value. The phenomenal growth of digital businesses like “digital platforms, artificial intelligence (AI), cloud computing, biometric identification, and data analytics has resulted in a completely new relationship between people, corporations, and government agencies”. In India, initiatives like “DigiLocker; Aadhaar; Digital India; CoWIN; UPI; and other e-governance platforms are facilitating the shift toward data-driven governance”. These efforts have improved government efficiency in delivering services and providing citizens with access to financial resources.¹ Citizens now experience more consistent, efficient delivery of government services, while increasing their participation in government.

However, these developments have raised serious concerns about individual privacy, surveillance, control over information and abuse of personal data.²

The emergence of the digital state has created substantial amounts of ‘personal data collected, stored, processed, and disseminated by government entities and the private sector’. Every time an individual interacts with a “service, whether through social media, internet banking, e-commerce, health services databases, or government portals, an active data trail is created by that interaction”. The length and extent of this data trail can be extensive enough to provide insights to an individual’s identity, lifestyle, habits, preferences, and familial and social relationship dynamics.³ As a result, ownership, control, and protection of personal data have become central issues in contemporary constitutional and legal discussions. The challenge for ‘privacy and data protection’ is particularly acute given the rapid digitalisation of India without there having been a ‘comprehensive data protection framework’ in place for such a long time.

Unlike many other jurisdictions, which enacted dedicated privacy and data protection laws from relatively early on, India relied on fragmented legal mechanisms to deal with privacy-related issues for decades. The legal basis for privacy protection has been established using

¹ “Digital India | Objectives, Key Initiatives & Progress,” *India Brand Equity Foundation* available at: <https://www.ibef.org/government-schemes/digital-india> (last visited June 3, 2026).

² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, First trade paperback edition (PublicAffairs, New York, NY, 2020).

³ Daniel Solove, “A Taxonomy of Privacy” *GW Law Faculty Publications & Other Works* (2006).

disparate sources: “the constitutional protections available; the provisions set out in the Information Technology Act of 2000; the regulations governing specific sectors; and the precedents established by the courts”.⁴ However, none of these measures have adequately addressed the complexities of contemporary digital ecosystems, which are defined by a variety of characteristics, including “algorithmic governance, cross-border data transfers, behavioural profiling and mass surveillance technologies”. Thus, due to the absence of an overall statutory framework, there existed an enormous legislative vacuum, where there were significant risks to citizens, but there was also significant discretion for both state and private actors in the handling of personal data.⁵

There was no doubt that the legislative vacuum was further highlighted through the expansion of Aadhaar and other large scale digital governance initiatives. While these programmes have been introduced in order to increase the efficiency of getting welfare assistance and making welfare assistance available, ‘concerns have also been raised in relation to the adequacy of consent given; whether the collections of data have been undertaken for legitimate purposes; whether there is proportionality between the use of data and the purpose for which it is collected; whether less data could have been collected; and whether or not there are appropriate mechanisms in place to hold actors accountable for their actions in relation to the collection and use of data’. In the absence of any specific legislative provisions that provide safeguards, the courts are frequently called upon to decide disputes regarding ‘privacy and surveillance, as well as the rights associated with having information about you’. Accordingly, it has been the role of the Indian judiciary to have played a significant role in developing privacy jurisprudence, and creating constitutional principles that can be used to regulate this digital sphere of activity.⁶

The approach taken by the judiciary in addressing these issues can be seen as a continuation of the broader trend of constitutional activism that has emerged in relation to ‘the protection of fundamental rights, in light of the changing social and technological context’. The Indian courts have made “privacy a fundamental right - by interpreting Article 21 of the Constitution of India in a broad manner. Judicial decisions, therefore, have not only dealt with immediate

⁴ “Data protection laws in India - Data Protection Laws of the World,” *available at*: <https://www.dlapiperdataprotection.com/?t=law&c=IN> (last visited June 3, 2026).

⁵ Graham Greenleaf, “Promises and illusions of data protection in Indian law,” 1 *International Data Privacy Law* 47–69 (2011).

⁶ Anupam Chander and Uday P. Laxar, “Data Nationalism.”

controversies; they have also established normative standards with respect to the collection of data, the practice of surveillance, and the right to self-decide about one's own information".⁷ The first time that privacy was recognised as a fundamental right occurred in the "case of Justice K.S. Puttaswamy v. Union of India and this case has established a constitutional right that serves as a key basis for the implementation of contemporary reforms in the area of data protection"⁸.

In light of this context, the present research will 'evaluate the role of the Indian courts in filling the legislative voids in relation to data privacy in the digital age'. In addressing this aim, 'the study will analyse how the process of judicial activism has contributed to the constitutionalisation of privacy, how this has influenced legislative developments, and how the emerging framework for digital governance in India will be shaped by this process'. In order to achieve this aim, the study will adopt a doctrinal and analytical methodology and rely on constitutional law materials, judicial decisions, legislative materials, and academic writings to determine the continuing significance of judicial intervention to protect privacy and sovereignty over information in an increasingly data-driven society.

Evolution of Privacy Jurisprudence in India: From Personal Liberty to Informational Privacy

The development of 'privacy jurisprudence in India is an outstanding case of developing a constitutionally protected right through judicial interpretation, since privacy is not stated explicitly within the Constitution and, unlike most modern constitutions, the Constitution of India does not include a specific provision for the right to privacy'. As a result, the development of privacy rights has occurred through creative judicial interpretation of Article 21, which protects life and personal liberty. Over time, *"the Supreme Court would establish privacy as something more than a peripheral issue and establish it as a constitutionally protected right, culminating with the establishment of constitutional rights regarding informational privacy in the digital age"*.

The earliest engagement with privacy can be found in *"M.P. Sharma v. Satish Chandra, the Supreme Court heard arguments from an 8-judge panel regarding the constitutionality of*

⁷ "Committee Report on Draft Personal Data Protection Bill, 2018_0.pdf,."

⁸ "Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017,"available at: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026).

search and seizure powers under the criminal procedures related to investigation".⁹ The Supreme Court ruled that 'the Constitution of India does not have a provision similar to the Fourth Amendment of the United States Constitution and therefore would not recognize privacy as a separate right under the Constitution'. This case is illustrative of the prevailing constitutional philosophy of the time that favored the interests of the state over the privacy interests of individual citizens. "*Kharak Singh v. The State of Uttar Pradesh is home to the Supreme Court's consideration of the constitutionality of police surveillance against a suspected criminal, in its decision, a majority of the Court held that there exists no independent right to privacy but that the constitutional guarantee of personal liberty was therefore violated by domiciliary visits during the night (art. 21 of the Constitution)*".¹⁰ The recognition of privacy, as articulated in a famous dissenting opinion by Justice Subba Rao, constituted a significant milestone in establishing an intellectual basis for the evolution of privacy-related violations.

The Court first began to redefine the law surrounding privacy in "*Gobind v. State of Madhya Pradesh, which broadly interpreted personal liberty; The Court did not find that a person's right to privacy could be absolute; however, the language of Articles 19 and 21 led the Court to infer that a right to privacy exists as part of an individual's constitutional protections*".¹¹ Justice Mathew's opinion created a pathway for the future establishment of privacy by suggesting that privacy would evolve as cases developed through the Courts.

In "*R. Rajagopal v. State of Tamil Nadu, otherwise known as the Auto Shankar Case, the Supreme Court expanded the concept of privacy to include the right to be let alone and established procedures for the proper disclosure of private information, unless there existed a legitimate public purpose to provide such information*".¹² In this way, the Supreme Court limited privacy to a right that included both informational and reputational interests, as against protecting privacy from physical invasion.

In "*PUCL v. Union of India, the Supreme Court was tasked with determining the*

⁹ "M. P. Sharma And Others vs Satish Chandra, District ... on 15 March, 1954,"available at: <https://indiankanoon.org/doc/1306519/> (last visited June 3, 2026).

¹⁰ "Kharak Singh vs The State Of U. P. & Others on 18 December, 1962,"available at: <https://indiankanoon.org/doc/619152/> (last visited June 3, 2026).

¹¹ "Govind vs State Of Madhya Pradesh & Anr on 18 March, 1975,"available at: <https://indiankanoon.org/doc/436241/> (last visited June 3, 2026).

¹² "R. Rajagopal vs State Of T.N on 7 October, 1994,"available at: <https://indiankanoon.org/doc/501107/> (last visited June 3, 2026).

constitutionality of the interception of an individual's telephone conversations in accordance with the provisions of the Indian Telegraph Act, 1885".¹³ The Supreme Court held that an individual's "right to privacy, as provided by article 21, was violated by arbitrary interception of a telephone call and provided for procedural safeguards governing the regulation of surveillance activities, thereby establishing the principle that an individual's privacy interests must be weighed against the state's legitimate interest in security".¹⁴

As a result of these judicial decisions addressing privacy rights, 'the judiciary has shifted privacy from a contested right to a fundamental right in the context of liberty established in the Indian Constitution'. With the continued proliferation of electronic devices, biometric data bases, and electronic communications, the law will continue to grow to encompass broader definitions of privacy that extend beyond protecting against physical invasions of privacy or communication. Moreover, *"informational privacy has emerged in response to the issues surrounding mass collection and use of data; specifically, informational privacy is the right of an individual to continue to control the collection, use, and dissemination, as well as the length of time for which personal information is retained"*.¹⁵

The progressive evolution of judicial definitions of privacy from 'M.P. Sharma v. Satish Kumar to PUCL has created the constitutional foundation for the landmark constitutional decision of Justice K.S. Puttaswamy v. Union of India (2017)'¹⁶. In Puttaswamy, 'the Supreme Court, sitting bench of nine judges, affirmed that the constitutional right to privacy is a fundamental right as guaranteed in the Constitution of India'. The Court held that the right to privacy constitutes three components: bodily privacy, decisional autonomously, and informational self-determination. As a result, 'the emergence of informational privacy represents the culmination of almost four decades of judicial inquiry and analysis into the intertwined concepts of liberty, dignity, and autonomy as established under the Constitution of India'.¹⁷

¹³ "People's Union Of Civil Liberties ... vs Union Of India (Uoi) And Anr. on 18 December, 1996," available at: <https://indiankanoon.org/doc/31276692/> (last visited June 3, 2026).

¹⁴ "Article 21 in Constitution of India," available at: <https://indiankanoon.org/doc/1199182/> (last visited June 3, 2026).

¹⁵ Gautam Bhatia, "The Supreme Court's Right to Privacy Judgment," 52 *Economic and Political Weekly* 22–5 (2017).

¹⁶ "M. P. Sharma And Others vs Satish Chandra, District ... on 15 March, 1954," available at: <https://indiankanoon.org/doc/1306519/> (last visited June 3, 2026); "People's Union Of Civil Liberties ... vs Union Of India (Uoi) And Anr. on 18 December, 1996," available at: <https://indiankanoon.org/doc/31276692/> (last visited June 3, 2026); "Kharak Singh vs The State Of U. P. & Others on 18 December, 1962," available at: <https://indiankanoon.org/doc/619152/> (last visited June 3, 2026).

¹⁷ Madhu Mainka, "Judicial Activism vs Judicial Overreach: A Critical Analysis of the Role of the Indian

Table 1: Evolution of Privacy Jurisprudence in India

Case	Year	Legal Issue	Contribution to Privacy Jurisprudence
<i>“M.P. Sharma v. Satish Chandra”</i>	1954	Search and seizure	Denied existence of a constitutional right to privacy
<i>“Kharak Singh v. State of U.P.”</i>	1963	Police surveillance	Recognized personal liberty concerns; dissent laid foundation for privacy rights
<i>“Gobind v. State of M.P.”</i>	1975	Surveillance regulations	Accepted privacy as an implied constitutional right under Articles 19 and 21
<i>“R. Rajagopal v. State of Tamil Nadu”</i>	1994	Publication of personal information	Recognized right to privacy and the "right to be let alone"
<i>“PUCL v. Union of India”</i>	1997	Telephone tapping	Protected communication privacy and established surveillance safeguards
<i>“Justice K.S. Puttaswamy v. Union of India”</i>	2017	Constitutional status of privacy	Declared privacy a fundamental right and recognized informational privacy

Judicial Activism and the Constitutionalization of Data Privacy

Judicial activism has become a significant feature of Indian constitutionalism, especially when the legislature and executive have been unsuccessful in guaranteeing fundamental rights. Generally, judicial activism refers to the proactive actions of the courts, which interpret constitutional provisions dynamically to respond to changing social realities and to ensure substantive justice. Judicial activism in India has been used as a method of filling legislative gaps, protecting vulnerable populations, and expanding the scope of constitutional guarantees. “The evolution of privacy jurisprudence is a prime example of how the judiciary has converted an unenumerated constitutional value into a fully enforceable fundamental right due to technological progress and legislative inaction”.¹⁸

The basis of the transformation of privacy jurisprudence lies in the expansive ‘judicial interpretation of Article 21’. Originally, “*Article 21 was interpreted narrowly in A.K. Gopalan v. State of Madras, where it only protected individuals from unlawful deprivation of life and*

Judiciary.”

¹⁸ Tom Zwart, “Review of Judicial Activism in India: Transgressing Borders and Enforcing Rights,” 30 *Journal of Law and Society* 332–7 (2003).

personal liberty”.¹⁹ However, the Supreme Court historic ruling in ‘Maneka Gandhi v. Union of India fundamentally changed this interpretation by ruling that the process required by law must be just, fair, and reasonable’.²⁰ This ruling established a process of transformative constitutional jurisprudence that has allowed “*Article 21 to serve as the basis for a variety of unenumerated rights, including dignity, livelihood, health, education, shelter, and privacy*”²¹. The courts have thus adopted purposive interpretations of constitutional rights, which have ensured that the Constitution continues to reflect ‘changing societal conditions’. With the emergence of privacy as a constitutional issue came rapidly advancing surveillance technologies, digital communication, and extensive data-based governance, making privacy concerns a prominent issue for the judiciary. Through various cases, including “*Gobind v. State of Madhya Pradesh*”²², *R. Rajagopal v. State of Tamil Nadu*²³, and *PUCL v. Union of India*”²⁴, the judiciary began to recognize privacy interests within the ambient interests of personal liberty. However, absent any definitive declarations regarding its constitutional basis led to uncertainty concerning the ‘nature and extent of privacy rights’. Ultimately, “*the Supreme Court of India resolved the ambiguity regarding privacy through its judgment in Justice K.S. Puttaswamy (Retired) v. Union of India*”²⁵, which many have viewed as a constitutional watershed moment for the development of Indian privacy law.

The context in which the “*Puttaswamy case arose was the myriad of challenges faced by the state with the implementation of the Aadhaar program and the imminent threat that arose through successful implementation would include large-scale collection of biometric data*”.²⁶ Recognising the grave implications that this issue posed to the citizens of India, the Supreme Court of India established a nine-member constitution bench to determine whether privacy represents a fundamental right protected under the Constitution of India. “*The Supreme Court*

¹⁹ “A.K. Gopalan vs The State Of Madras.Union Of India: ... on 19 May, 1950,”*available at*: <https://indiankanoon.org/doc/1857950/> (last visited June 3, 2026).

²⁰ “Maneka Gandhi vs Union Of India on 25 January, 1978,”*available at*: <https://indiankanoon.org/doc/1766147/> (last visited June 3, 2026).

²¹ “Article 21 of the Constitution of India: Understanding Right to Life and Personal Liberty from Case Laws - Academike,” 2024*available at*: <https://www.lawctopus.com/academike/article-21-of-the-constitution-of-india-right-to-life-and-personal-liberty/> (last visited June 3, 2026).

²² “Govind vs State Of Madhya Pradesh & Anr on 18 March, 1975,”*available at*: <https://indiankanoon.org/doc/436241/> (last visited June 3, 2026).

²³ “R. Rajagopal vs State Of T.N on 7 October, 1994,”*available at*: <https://indiankanoon.org/doc/501107/> (last visited June 3, 2026).

²⁴ “People’S Union Of Civil Liberties ... vs Union Of India (Uoi) And Anr. on 18 December, 1996,”*available at*: <https://indiankanoon.org/doc/31276692/> (last visited June 3, 2026).

²⁵ “Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017,”*available at*: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026).

²⁶ *Ibid*.

*heard the case and provided the citizens of India with unanimous opinions that privacy, as a right, is an aspect of the right to life and personal liberty conferred by Article 21*²⁷, and as a result must be afforded the protection of the freedoms guaranteed to all citizens by Part III of the Constitution.

The Supreme Court's judgment in 'Puttaswamy also expressly overruled prior judicial conclusions with respect to the right to privacy that were described as restrictive in M.P. Sharma and Kharak Singh'²⁸, thereby elevating 'the right of privacy to the level of constitutional protection, and also recognised the many facets of privacy as a constitutionally protected right'. One of the most essential provisions made by 'Puttaswamy was establishing that privacy is not only confined to physical space but also extends to informational privacy'. The Court held that in this digital age of constant interaction between individuals and the government, businesses, and various platforms creates a continuous flow of personal data. Thus, privacy also includes an individual's right over all aspects of their personal data, including how that data is collected, processed, stored, and distributed. This was a critical recognition since it creates a foundation under the Constitution for protecting data and providing a right to determine how personal data is used, which are necessary elements of contemporary privacy regulation throughout the world.²⁹

Additionally, the Court connected privacy with dignity and autonomy under the Constitution. The Court held that because privacy is necessary for an individual to develop fully as a person and exercise their free will, it allows an individual to make choices regarding their relationships, beliefs, identity, bodily integrity and how they want to share their information without arbitrary interference from either the State or private parties.³⁰ Therefore, the Court shifted privacy from a mere negative liberty to a substantive constitutional principle.

What has thus far been established regarding the role of judicial activism within privacy jurisprudence encompasses much more than simply the acknowledgment of rights. In effect,

²⁷ "Article 21 in Constitution of India," *available at*: <https://indiankanoon.org/doc/1199182/> (last visited June 3, 2026).

²⁸ "Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017," *available at*: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026); "Kharak Singh vs The State Of U. P. & Others on 18 December, 1962," *available at*: <https://indiankanoon.org/doc/619152/> (last visited June 3, 2026); "M. P. Sharma And Others vs Satish Chandra, District ... on 15 March, 1954," *available at*: <https://indiankanoon.org/doc/1306519/> (last visited June 3, 2026).

²⁹ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, Oxford, GB, 2015).

³⁰ Gautam Bhatia, "The Supreme Court's Right to Privacy Judgment," 52 *Economic and Political Weekly* 22–5 (2017).

the judiciary has bridged a legislative gap that existed for decades, notwithstanding the growing demand for protection of personal data. Before enactment of ‘the Digital Personal Data Protection Act, 2023, judicial rulings were primarily responsible for affording privacy protection in India’. The courts created rules relating to consent, informational authority, oversight of surveillance, and (to some degree) constitutional accountability, laying the foundation for the normative framework on which future legislation will be based. Thus, through judicial activism, the legislature was effectively stimulated to undertake legal action to reform existing laws and modernize the Constitution.

Judicial intervention's constitutionalization of privacy has ignited debate around the appropriate limitations of judicial authority. Critics assert that intrusive judicial activism may frustrate democratic accountability by intruding into the sphere of elected bodies.³¹ Proponents of judicial intervention argue that it is warranted whenever legislative inaction threatens to undermine essential rights and constitutional values. In the area of data privacy specifically, ‘the judiciary's proactive approach is viewed as crucial due to the lack of a cohesive legal framework governing this area, coupled with the continual development of digital technologies that present increased dangers’.³²

Table 2: Judicial Activism and Constitutionalization of Privacy

Constitutional Development	Judicial Contribution	Impact on Data Privacy
Expansion of Article 21	<i>Maneka Gandhi</i> broadened personal liberty	Enabled recognition of unenumerated rights
Recognition of Privacy Interests	<i>Gobind, Rajagopal, PUCL</i>	Established privacy as part of personal liberty
Fundamental Right Status	<i>Puttaswamy</i> (2017)	Declared privacy a fundamental right
Informational Privacy	<i>Puttaswamy</i>	Constitutional basis for data protection
Dignity and Autonomy	<i>Puttaswamy</i>	Linked privacy with individual self-determination

³¹ “Proportionality: Constitutional Rights and their Limitations,” available at: https://www.researchgate.net/publication/288220537_Proportionality_Constitutional_rights_and_their_limitations (last visited June 3, 2026).

³² IJLLR Journal, “The Role Of Judicial Activism In Expanding Privacy Rights In India: An Analysis” *IJLLR Journal*, 2024 available at: <https://www.ijllr.com/post/the-role-of-judicial-activism-in-expanding-privacy-rights-in-india-an-analysis> (last visited June 3, 2026).

Constitutional Development	Judicial Contribution	Impact on Data Privacy
Proportionality Doctrine	<i>Puttaswamy</i>	Constitutional test for privacy restrictions
Legislative Influence	Judicial precedents	Influenced DPDP Act, 2023 and future privacy regulation

Filling Legislative Lacunae: Judicial Responses to Data Governance Challenges

Indian courts developed substantive safeguards of privacy before Parliament's comprehensive data protection legislation and established many of the constitutional principles required to construct current data protection legislation in India's judiciary through challenges to various digital governance issues. These issues included the 'emergence of digital governance challenges and biometric identification systems, state surveillance of individuals, and the power of technology platforms. Courts responded to the newly developing challenges of digitisation by responding to these problems and filling a large legislative void and establishing substantial constitutional foundations for contemporary data protection legislation.

Considering the large-scale litigation regarding Aadhaar, it is easy to provide an example of the judiciary developing principles as a result of the litigation related to Aadhaar through significant court cases. As a biometric identity system, 'Aadhaar was intended to simplify the delivery of government welfare through identifying individuals by creating a repository of the individual's comprehensive demographic and biometric data'.³³ There were immediate concerns about the hypersensitivity of people with respect to their data, including concerns regarding data security, surveillance, profiles of people's biometrics, and the lack of legislative safeguards. As a result of these concerns, 'a large number of petitions were filed with the Supreme Court challenging the constitutionality of Aadhaar and the ability of the government to create a structure to collect and store individual biometric data on this scale'.³⁴

Similarly, the emergence of new 'digital platforms such as social media companies', search engine companies and intermediaries, has created new regulatory challenges. 'Social media companies, search engines and intermediary platforms are able to collect vast amounts of personal data while exercising a significant degree of discretion over how communications are

³³ "Aadhaar Act 2016 as amended.pdf,."

³⁴ "Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017,"available at: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026).

conducted on their platforms’.³⁵ The courts have begun to adjudicate cases concerning intermediary liability and the freedom of expression on the Internet as well as the accountability of those companies. There have been a variety of factors that have influenced decisions with respect to content moderation, traceability and user rights. In many cases, the courts represent the principal means to resolve issues that result from the digital regulation of technologies until comprehensive laws exist.

The judicial creation of privacy standards in the absence of statutory regulations represents the single greatest contribution of the courts to the right to privacy. In several cases, ‘including Gobind v. State of Madhya Pradesh, R. Rajagopal v. State of Tamil Nadu, PUCL v. Union of India and Puttaswamy’³⁶, the Supreme Court has established a series of principles to recognize that individuals have a right to their personal data protected by (1) autonomy, (2) consent, (3) dignity and (4) control. These principles established by the Supreme Court were a preview of many principles that would eventually become part of comprehensive data protection legislation such as limited purpose, informed consent and accountability.

In essence, the courts have acted as de facto regulators of data protection in India during a time when no data protection legislation has existed. Rather than simply resolving individual disputes, ‘the courts have established constitutional norms regarding how to collect, process and use personal information’.³⁷ The courts have established a coherent constitutional framework for privacy which establishes rules to address the problems presented by new technologies. Judicial activity regarding ‘the protection of individual rights provides the foundational norms to support future legislation that will provide a stable, reliable form of data protection; specifically, the Digital Personal Data Protection Act, 2023’³⁸.

³⁵ Apar Gupta, “Privacy is a solution” *Blackletter*, 2017 available at: <https://medium.com/aparatbar/privacy-is-a-solution-de44b092563d> (last visited June 3, 2026).

³⁶ “A.K. Gopalan vs The State Of Madras.Union Of India: ... on 19 May, 1950,” available at: <https://indiankanoon.org/doc/1857950/> (last visited June 3, 2026); “Govind vs State Of Madhya Pradesh & Anr on 18 March, 1975,” available at: <https://indiankanoon.org/doc/436241/> (last visited June 3, 2026); “Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017,” available at: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026); “Kharak Singh vs The State Of U. P. & Others on 18 December, 1962,” available at: <https://indiankanoon.org/doc/619152/> (last visited June 3, 2026); “M. P. Sharma And Others vs Satish Chandra, District ... on 15 March, 1954,” available at: <https://indiankanoon.org/doc/1306519/> (last visited June 3, 2026).

³⁷ Priya Prabhakar, “Tracing Biometric Assemblages in India’s Surveillance State: Reproducing Colonial Logics, Reifying Caste Purity, and Quelling Dissent Through Aadhaar.”

³⁸ “2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf,”

From Judicial Innovation to Legislative Action: Impact on the DPDP Act, 2023

“The Digital Personal Data Protection Act, 2023 (DPDP Act)”, is the result of a constitutional and judicial journey in the realm of privacy law in India. The enactment of the ‘DPDP Act marks the end of a long and arduous legal journey toward establishing a legal foundation for individual privacy rights. Unlike many jurisdictions where privacy rights were first recognized as constitutional rights prior to the establishment of a legislative framework for privacy law, the legal journey in India has been the reverse of this approach. Thus, through judicial innovation by way of expansive constitutional interpretation, the courts have created the normative foundations upon which a contemporary data protection regime has developed in India. In this way, ‘the DPDP Act is a consequence of judicial decision-making that articulates privacy as a fundamental constitutional value, as well as being a legislative response to developments in technology that require a legal framework’.

The immediate catalyst ‘for the enactment of a data protection law was the Supreme Court's landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India’.³⁹ There, ‘the Supreme Court of India found that privacy is an inherent part of dignity, liberty, and autonomy under Article 21 of the Indian Constitution’⁴⁰ and thus the State has a constitutional duty to protect the information of an individual from arbitrary encroachment. In that ruling, “*the Supreme Court specifically found that informational privacy is an important aspect of personal freedom, and that there is a need for a complete legal framework for data processing*”. In addition, the constitutional requirements set out in Puttaswamy helped to move along discussions related to data protection, digital governance, and policy development much faster than would have occurred without the judgment.

In response to ‘*the Supreme Court's decision in the Puttaswamy case, the Government of India established the Expert Committee to Create a Data Protection Law, by appointing a Chairperson, Justice B.N. The Panel was constituted on 1 July 2020, under the chairmanship of Justice Srikrishna, to assess the challenges of data protection and data privacy*’.⁴¹ One of the most significant documents in the debate surrounding privacy law in India was the Committee’s report titled “Free and Fair Digital Economy: Protecting Privacy and

³⁹ “Justice K.S. Puttaswamy (Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017,” available at: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026).

⁴⁰ “Article 21 in Constitution of India,” available at: <https://indiankanoon.org/doc/1199182/> (last visited June 3, 2026).

⁴¹ “Committee Report on Draft Personal Data Protection Bill, 2018_0.pdf.”

Empowering Indians” (the “Srikrishna Report”). The Srikrishna report made extensive use of constitutional legal principles identified in the ‘Puttaswamy case and comparative models of data protection, including the EU’s General Data Protection Regulation (GDPR), to propose a comprehensive rights-based data protection framework’.

The recommendations of the “Srikrishna Report laid the foundation for the Personal Data Protection Bill, 2019, which was India’s first comprehensive attempt at regulating the processing of personal data”.⁴² The Bill proposed several data protection mechanisms that enhanced privacy, such as rights of individuals to access and correct their information; the right to portability and deletion of their personal data; and obligations on data custodians to be accountable for their data handling activities. Following extensive public debate and criticism of the Bill, it was ultimately withdrawn in 2022 and replaced with a new legislative framework.

The DPDP Act, 2023 now serves as ‘the regulatory framework for the protection of personal data in India’. Many provisions in the Act can be traced to previous judicial decisions or through the work of various committees prior to the Act being established. Among other things, “the DPDP Act recognizes the role of consent in personal data processing; imposes obligations on data custodians; confers rights of individuals to protect their personal data; and establishes a process for the resolution of complaints and enforcement of the Act”.⁴³ These provisions also represent the constitutional ‘values of dignity, autonomy and control over information, which were established in the Puttaswamy judgment’. The DPDP Act also recognizes the importance of the protection of personal data to ensure an individual’s freedom in a digital society.

Despite the advances represented by the DPDP Act, there are significant gaps between the aspirational constitutional values and the actual legislative implementation of data protection laws. One of the most significant issues identified by stakeholders is the broad exemptions from regulatory oversight that data custodians receive from governmental or other public entities under specified circumstances.⁴⁴ Critics of the exemptions argue that they will dilute the application of the principles of proportionality established by the Supreme Court and create opportunities for excessive government surveillance. Other areas of concern relate to “the lack of detailed protections for sensitive personal data, insufficient criteria for automated decision

⁴² “4173LS(Pre).p65,.”

⁴³ Graham Greenleaf, “Promises and illusions of data protection in Indian law,” 1 *International Data Privacy Law* 47–69 (2011).

⁴⁴ Gautam Bhatia, “The Supreme Court’s Right to Privacy Judgment,” 52 *Economic and Political Weekly* 22–5 (2017).

making and the absence of an independent regulatory authority”.⁴⁵

Continuing Gaps in the Digital Personal Data Protection Framework and the Future Role of Courts

While the “Digital Personal Data Protection Act, 2023 represents a significant shift in the field of privacy rights within India, it still faces many limitations and restrictions under the constitution and through the institutions that develop and implement laws in India”. The development of a statutory framework does not automatically provide a solution to the data governance problems facing Indian citizens today, especially when we consider “artificial intelligence; algorithm-driven decision-making processes; and the use of biometric data and cross-border data transfers”. Courts will likely continue to play an important role in ensuring that the protection of privacy follows the principles of dignity, autonomy, accountability, and proportionality set out in the constitutional framework.

One of the most contentious provisions in the DPDP Act is the expansive exemptions from compliance with the Act for government agencies. The Act gives the ‘Central Government the authority to grant exemptions from compliance with key requirements of the Act for certain government agencies based upon grounds such as sovereignty, national security, public order, and preventing the commission of offences.

There are also significant problems with the current construct of the legal system regarding the rapid advancements in artificial intelligence and the use of algorithmic governance. Public and private entities, for example, “are increasingly relying on automated systems to determine employment, the creditworthiness of applicants, health care, policing, and the distribution of welfare”.⁴⁶ These systems operate using algorithms that produce opaque results, and will almost always result in bias, discrimination, or arbitrary decision making.⁴⁷

Another area of potential uncertainty involves cross-border data transfers and their legality. The digital economy relies on the movement of data across international borders, but these transfers raise concerns surrounding regulatory fragmentation, jurisdictional conflicts, and privacy protection standards.⁴⁸ While the DPDP Act provides some clarity around cross-border

⁴⁵ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, Oxford, GB, 2015).

⁴⁶ Rowena Rodrigues, “Legal and human rights issues of AI: Gaps, challenges and vulnerabilities,” 4 *Journal of Responsible Technology* 100005 (2020).

⁴⁷ Alexandra Jonker Rogers Julie, “What Is Algorithmic Bias? | IBM,” 2024 available at: <https://www.ibm.com/think/topics/algorithmic-bias> (last visited June 3, 2026).

⁴⁸ “Cross-Border Data Transfers and Data Localization Mandate under the Data Protection Regime,” available

data transfers, there remain unanswered questions regarding standards for determining adequacy, data localization, and how Indian citizen's data will be protected while processed outside of India.

Additionally, the importance of constitutional oversight carries weight in future cases, as indicated in the Puttaswamy decision. The Supreme Court found, “as a fundamental right, that privacy is not simply a statutory right, but a right that is a critical component of dignity, liberty, and democratic citizenship”.⁴⁹ Thus, legislative and executive actions should continue to be subject to constitutional review by the judiciary.

Therefore, the role of the courts in India as guardians of digital constitutionalism is on the rise. Digital constitutionalism applies constitutional principles and values to the technological age ‘to protect the individual from both the state and private sources of power’.⁵⁰ Courts must therefore ensure that the advancement of digital technologies does not erode constitutional freedoms.

Thus, both continued legislative improvement and constitutional vigilance are necessary for the future of privacy protection in India. While the DPDP Act establishes the foundation for a regulatory framework, its success will be determined by the courts' interpretation and enforcement of it. As a result, courts must continue to act as guardians of the Constitution and ensure that technological advancement is consistent with democratic ideals, individual autonomy, and the rule of law.

Conclusion

The development of data privacy legislation in India represents the powerful impact of judicial interpretation in furthering the protection of constitutional rights in a society that has become more digitalized. In the absence of comprehensive statutory law, ‘the courts in India have, over time, created an expanding scope of Article 21⁵¹ and developed a complex body of privacy law grounded in dignity, autonomy, liberty, and self-determination regarding information’. The Supreme Court recognized the ‘right to privacy as a fundamental right held by individuals when

at: <https://vidhilegalpolicy.in/blog/cross-border-data-transfers-and-data-localization-mandate-under-the-data-protection-regime/> (last visited June 3, 2026).

⁴⁹ Vrinda Bhandari et al., “An Analysis of Puttaswamy: The Supreme Court’s Privacy Verdict.”

⁵⁰ “Digital Constitutionalism, Challenges, Legal Framework in India & Global,” *available at*: <https://vajiramandravi.com/current-affairs/digital-constitutionalism/> (last visited June 3, 2026).

⁵¹ “Article 21 in Constitution of India,” *available at*: <https://indiankanoon.org/doc/1199182/> (last visited June 3, 2026).

it issued its ruling in *K.S. Puttaswamy v. Union of India*⁵²; the pronouncement is widely viewed as the watershed moment that set the stage for the passage of the “Digital Personal Data Protection Act, 2023”.

While the DPDP Act is intended to achieve the constitutional goal established by the Supreme Court, there are several significant gaps in the law that can threaten the rights of individuals. These include expansive government exceptions under the Act, an insufficiently independent and autonomous Data Protection Authority, a lack of procedural protections against algorithmic decision-making, and inadequate opportunities for oversight.

Thus, future reforms to digital governance must adopt a rights-based framework. ‘An independent Data Protection Authority with sufficient budgetary and functional independence is necessary to promote greater enforcement and public confidence in the DPDP Act’. All public surveillance systems should require a proportionality review process and independent judicial authorization before implementation. Any legislative reform must provide for accountability concerning algorithmic decision-making by requiring transparency in algorithm operation, conducting an impact assessment of the effect of ‘algorithmic decision-making on individuals, and providing individuals with a sufficient explanation of any automated decision-making process’.

Additionally, the interpretation of the right to privacy must be citizen-centered—i.e., focused on ensuring an individual provides informed consent before their ‘personal information is collected, used for any purpose beyond that for which it was collected, and that they have meaningful control over their personal information’.

Ultimately, the success of the digital governance framework in India will reflect the increasing interdependence and interaction between constitutional principles and technological innovation. Courts must remain vigilant in their role as guardians of the digital constitutionalism movement to ensure that technological advancement serves democratically supportive values, rather than undermining them. Achieving this goal will require adopting an effective privacy framework based on constitutional accountability, institutional independence, and respect for the individual autonomy of every Indian citizen in a digital world.

⁵² “Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017,”*available at*: <https://indiankanoon.org/doc/91938676/> (last visited June 3, 2026).

BIBLIOGRAPHY

BOOKS

1. Lyskey, Orla, *The Foundations of EU Data Protection Law* (Oxford University Press, Oxford, 2015).
2. Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, New York, 2020).

JOURNAL ARTICLES / RESEARCH PAPERS

1. Bhandari, Vrinda et al., “An Analysis of Puttaswamy: The Supreme Court’s Privacy Verdict.”
2. Bhatia, Gautam, “The Supreme Court’s Right to Privacy Judgment” (2017) 52 *Economic and Political Weekly* 22.
3. Chander, Anupam and Uyên P. Lê, “Data Nationalism.”
4. Greenleaf, Graham, “Promises and Illusions of Data Protection in Indian Law” (2011) 1 *International Data Privacy Law* 47.
5. Mainka, Madhu, “Judicial Activism vs Judicial Overreach: A Critical Analysis of the Role of the Indian Judiciary.”
6. Prabhakar, Priya, “Tracing Biometric Assemblages in India’s Surveillance State: Reproducing Colonial Logics, Reifying Caste Purity, and Quelling Dissent Through Aadhaar.”
7. Rodrigues, Rowena, “Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities” (2020) 4 *Journal of Responsible Technology* 100005.
8. Solove, Daniel J., “A Taxonomy of Privacy” (2006) GW Law Faculty Publications & Other Works.
9. Zwart, Tom, “Review of Judicial Activism in India: Transgressing Borders and Enforcing Rights” (2003) 30 *Journal of Law and Society* 332.

CASES

1. *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.
2. *Govind v. State of Madhya Pradesh*, AIR 1975 SC 1378.

3. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
4. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
5. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
6. *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
7. *People's Union for Civil Liberties v. Union of India*, AIR 1997 SC 568.
8. *R. Rajagopal v. State of Tamil Nadu*, AIR 1995 SC 264.

GOVERNMENT REPORTS / COMMITTEE REPORTS

1. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Report on the Draft Personal Data Protection Bill, 2018).

STATUTES

1. Constitution of India, 1950.
2. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

WEBSITES

1. Apar Gupta, "Privacy is a Solution" (2017), available at: <https://medium.com/aparatbar/privacy-is-a-solution-de44b092563d> (visited on June 3, 2026).
2. DLA Piper, "Data Protection Laws in India", available at: <https://www.dlapiperdataprotection.com/?t=law&c=IN> (visited on June 3, 2026).
3. IBM, "What is Algorithmic Bias?" (2024), available at: <https://www.ibm.com/think/topics/algorithmic-bias> (visited on June 3, 2026).
4. India Brand Equity Foundation, "Digital India: Objectives, Key Initiatives and Progress", available at: <https://www.ibef.org/government-schemes/digital-india> (visited on June 3, 2026).
5. IJLLR Journal, "The Role of Judicial Activism in Expanding Privacy Rights in India: An Analysis" (2024), available at: <https://www.ijllr.com/post/the-role-of-judicial-activism-in-expanding-privacy-rights-in-india-an-analysis> (visited on June 3, 2026).

6. Lawctopus, “Article 21 of the Constitution of India: Understanding Right to Life and Personal Liberty from Case Laws” (2024), available at: <https://www.lawctopus.com/academike/article-21-of-the-constitution-of-india-right-to-life-and-personal-liberty/> (visited on June 3, 2026).
7. Vajiram & Ravi, “Digital Constitutionalism: Challenges, Legal Framework in India and Globally”, available at: <https://vajiramandravi.com/current-affairs/digital-constitutionalism/> (visited on June 3, 2026).
8. Vidhi Centre for Legal Policy, “Cross-Border Data Transfers and Data Localization Mandate under the Data Protection Regime”, available at: <https://vidhilegalpolicy.in/blog/cross-border-data-transfers-and-data-localization-mandate-under-the-data-protection-regime/> (visited on June 3, 2026).