



JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1, Issue 2

Article 2

How Safe Is Your Data? Understanding Digital Privacy Rights in India

Akanksha Singh

Jagran Lakecity University

Recommended Citation:

Singh (2026) “How Safe Is Your Data? Understanding Digital Privacy Rights in India” Journal of Cyber Governance and Intellectual Property, Vol. 1, Issue 2, Article 2. (DOI)

This article is published under the Creative Commons Attribution–NonCommercial–ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows for free non-commercial use, distribution, and reproduction in any medium, provided appropriate credit is given to the original work.

ABSTRACT

Today's technology driven society people communicate, shop, work, avail services differently due to the ever-increasing digitalization. As usage of internet, mobile and digital India projects is growing exponentially people's data is collected and made available to various people for usage. Issues surrounding people's right to privacy, unauthorised access, cybercrime, misuse of information and privacy concerns surrounding private bodies become important. Though measures have been put in place laws and regulation issues still exist about its implementation, awareness and accountability. The paper examines India's digital privacy rights, existing and emerging challenges like informed consent, growing data breaches, government's responsibility, in a world defined by the growing internet and digital evolution. The paper also underlines loopholes that exist between legal safeguards meant to safeguard the digital rights and the ground reality and the need to evolve stronger enforcement actions complemented by enhanced digital literacy and awareness with greater transparency in data handling practices to protect every individual's digital rights & freedom in India.

KEYWORDS

Right to privacy, Freedom, Legal safeguards, Cybercrime, Government's responsibility, Digitalization

INTRODUCTION

The acceleration of technology in India has had a drastic impact on day-to-day activities. Services have expanded to online banking, digital payments, online shopping and social media, digital healthcare, and e-government.¹ People are comfortable using technology to share personal information. Projects like Digital India have increased the pace of the use of technology and the provision of government services online.

The reliance on technology has sparked complex issues of personal data protection. Data breaches, the theft of identity, digital crimes, and illegal surveillance and use of private data have shown the need to protect the right to privacy in the digital world.

The case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) was a major advancement in the Indian right-to-privacy case law. The Supreme Court recognized the right to privacy as part of the right to life and personal liberty under Article 21 of the Constitution.² This was soon followed by the Digital Personal Data Protection Act, 2023.³ This protects individuals' digital personal data, and places restrictions on the use of digital personal data. Even with the introduction of this law, issues remain regarding the actual use of this law, lack of knowledge, and the lack of responsible implementation and enforcement of data protection laws.⁴

Research Problem

Even with India's constitutional and statutory provisions designed to protect digital privacy, practical issues have made these provisions mostly ineffective. Many people do not know the means by which government and privately owned companies collect, process, store, or sell their personal data. A big disconnect between data protection laws and their enforcement is obvious due to repeated data breaches and cyber-attacks, and problems with transparency and informed consent. Because of these issues, the following question must be asked: Do the existing laws and regulations provide adequate protection of the digital privacy of the individuals of India?

¹ Digital India Programme, <https://www.digitalindia.gov.in> (last visited Jul. 5, 2026).

² Supreme Court Observer, <https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/> (last visited Jul. 5, 2026).

³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁴ Ministry of Electronics & Information Technology (MeitY), *Acts and Policies*, <https://xn--m1bdba5a7gresc7dsa.xn--11b7cb3a6a.xn--h2brj9c/documents/act-and-policies?page=1> (last visited Jul. 5, 2026).

Research Objectives

- To examine the relevance and significance of digital privacy rights in India.
- To analyze the constitutional and legal data protection systems.
- To assess the primary barriers to the enforcement of digital privacy legislation.
- To assess the obligations of the Government and the private sector in the safeguarding of digital privacy.
- To recommend ways to protect digital privacy and to improve enforcement and public education.
- To assess how well the current laws and regulations in India protect the digital privacy of individuals.

This paper analyses the digital privacy rights of individuals in the Constitution of India and the data protection legislation of India, the implementation barriers, the protection gaps, and proposes ways to strengthen the safeguard of digital rights in a technology-dominated world.

LITERATURE REVIEW

The combination of rapidly developing technologies and a growing trend of data collection has propelled digital privacy to the forefront of legal and scholarly research.⁵ Most of the research focuses on privacy, the evolution of data protection in India, and the efficacy of the Digital Personal Data Protection Act, 2023 (DPDP Act). While these studies analyze the legal structures, they simultaneously identify numerous implementation, oversight, and enforcement gaps in protecting the digital rights of individuals.⁶

The most significant case for establishing digital privacy in India is the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017).⁷ The Supreme Court of India identified the Right to Privacy as a fundamental right deriving from the right to life and personal liberty

⁵ Charu Malhotra, *Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India*, 70 Sage Journals. 516, 531 (2024)
<https://journals.sagepub.com/doi/10.1177/00195561241271575>. (last visited Jul. 5, 2026)

⁶ Mahindra Singh Hanspal, *The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions*, 6 ResearchGate. 12, 21 (2025)
https://www.researchgate.net/publication/400280418_The_Digital_Personal_Data_Protection_Act_2023_Key_Provisions_Issues_and_Future_Directions. (last visited Jul. 5, 2026)

⁷ Akshat Jain, *Tracing the Constitutional Journey of Data Privacy in India: From Puttaswamy to the Draft DPDP Rules, 2025*, SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5283949. (last visited Jul. 5, 2026, 02:43 PM)

(Article 21). This case is the first in the legal history of India to recognize the importance of privacy in the context of the dignity and the autonomy of individuals. The majority of studies that focus on data protection frameworks in India cite this case to explain the right to privacy and the responsibility of the State to protect personal data.

The Digital Personal Data Protection Act, 2023 is India's first all-encompassing law on digital personal data protection. Malhotra and Malhotra write about features like data fiduciaries and the emphasis on individuals maintaining control over their personal data. They identify a number of issues related to the ability of the State to implement the Act, as well as the awareness of citizens.

In a similar vein, Chesta's study on the evolution of the DPDP Act shows that India's data protection framework has built up through the interpretation of the Constitution, many drafts of legislation, and policy changes, before the 2023 legislation. The study argues the Act shows considerable legislative advances, though it will be subject to further changes as emerging technologies will require additional implementational safeguards.

The DPDP Act has come in for considerable scholarly criticism focusing on its strengths and weaknesses.⁸ Kumar and his co-researchers suggest that even though the Act has laid down a critical regulatory framework, broad governmental exemptions, the Data Protection Board's independence, and the Act's enforcement opacity, among others, are considerable concerns. Others similarly argue that the Act needs improved enforcement mechanisms and that arbitrary data collection and surveillance in the Act must be constrained.⁹

Studies have examined the enforcement of privacy legislation across different sectors. Bareh, in his study of Libraries, argues that the DPDP Act, while framed in the context of libraries, addresses the privacy concerns of data related to consent, processing, retention, security, and user rights. While this study is framed in the context of a library, it illustrates the enforcement challenges faced by various sectors which will be impacted by data protection.

⁸ Mahindra Singh Hanspal, *The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions*, 6 ResearchGate. 12, 21 (2025)
https://www.researchgate.net/publication/400280418_The_Digital_Personal_Data_Protection_Act_2023_Key_Provisions_Issues_and_Future_Directions. (last visited Jul. 5, 2026)

⁹ Abhishek Kumar, *India's New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023*. 44 Library Progress International. 11776, 11780 (2024)
<https://bpasjournals.com/library-science/index.php/journal/article/view/2513>. (last visited Jul. 5, 2026)

Recent studies examine the bounds on State data collection on the basis of the constitution and the challenges of automated AI-driven profiling.¹⁰ These studies claim the DPDP Act is a major step in the right direction, but leaves the issues of algorithmic adjudication, AI in its forms, and the Puttaswamy case's proportionality doctrine unaddressed. These studies call for increased regulation and protective mechanisms against the threats to the citizens of a developing digital world.

Nevertheless, a large number of gaps remain in the literature. Most of the literature is focused on the analysis of the statutory provisions of the DPDP Act or the constitutional theories of the adjudicated cases. Comparatively, fewer studies analyze the challenges and the protection of the rights of citizens in the digital environment. Limited digital literacy, informed consent, difficulties in the enforcement of the law, and a lack of social accountability and awareness remain empirical gaps. The gap is also large in the analysis of the legal protection of rights and the real digital environment used by citizens.

The present research aims to cover these gaps. This study analyzes the digital privacy of citizens in India by combining the challenges of digital protection with the enforcement of the rights of citizens, constitutional values, and the statutory provisions. This study is an attempt to strengthen the protection of digital privacy of citizens in India.

RESEARCH METHODOLOGY

The study adopts a doctrinal approach involving the examination of legal documents and sources, as opposed to the collection of empirical data. This methodology is suitable for the research as it seeks to understand the existing laws concerning digital privacy in India and their deficiencies in enforcement.

Both primary and secondary sources are used in this study. The primary sources are the Constitution of India (especially Article 21), the Digital Personal Data Protection Act, 2023, the Indian Information Technology Act, 2000, and important case law, especially Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). These cases are important to assess the privacy of the Constitution of India and the law concerning the collection and safeguarding of personal data.

¹⁰ Abhinav Singh, *Automated Profiling, Privacy Rights, and Gaps in India's DPDP Act 2023*, 9 IRE Journals. 3521, 3527 (2026) <https://www.irejournals.com/paper-details/1717032>. (last visited Jul. 5, 2026)

The secondary sources include books, articles in peer-reviewed journals, legal research papers, government reports, reports of different committees, policy documents, legitimate online legal research tools, and more. The development of the law concerning digital privacy and the problems of digital data protection are assessed through the extensive critique and recommendation literature concerning the contemporary problems of consent, cybercrime, and accountability.

The study employs an analytical and a descriptive approach. The descriptive approach illustrates the present legal structure and the evolution of the judiciary. In contrast, the analytical approach identifies the merits and demerits of the legislations and policies concerning digital privacy. Relevant cases and statutes have been analyzed with the constitutional provisions and with the advanced technology of the present day.

The research aims to study the legal position of digital privacy rights in India alone. It does not include field surveys, interviews, questionnaires, or any other empirical methods. It aims to offer a critique of legal theories and frameworks in order to ascertain the sufficiency of the existing legal framework in the protection of individuals' digital privacy and to recommend the necessary provisions for the protection of individuals' digital privacy and the mechanisms for its enforcement.

CONSTITUTIONAL FOUNDATION OF DIGITAL PRIVACY RIGHTS IN INDIA

Even without a specific declaration of the privacy right in the Indian Constitution, judicial interpretation has distinguished the right to privacy within the scope of the right to life and personal liberty of Article 21. The relevance of privacy as a right within the framework of the Constitution has gained further significance, with the phenomenal growth of digital technologies and services, AI and e-governance.

Privacy was initially viewed narrowly by the Supreme Court. In *M.P. Sharma v. Satish Chandra* (1954), the Court held that a right to privacy was not conferred by the Constitution.¹¹ In *Kharak Singh v. State of Uttar Pradesh* (1962), the majority also refused to accept privacy as an independent fundamental right.¹² However, in the following years, the scope of Article

¹¹ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

¹² *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

21 was expanded by the courts as the right to life was interpreted to include the right to live with dignity,¹³ and the right to personal liberty.¹⁴

A landmark moment occurred in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) when a nine-judge Constitution Bench ruled in a landmark verdict that the right to privacy is a basic right enshrined in Part III of the Constitution and all nine judges voted in favor of this ruling.¹⁵ The Court opined that the right to privacy is critical to the dignity of the individual, the right to self-determination, and the right of an individual to make choices freely. The Court also observed that the right to privacy under the Constitution also includes the right to privacy of information, which relates to the worry of the collection, retention, and utilization of one's personal information. The judgment also noted that the constant innovation in technology has equipped both the State and private entities to collect and process huge volumes of personal information and that the absence of appropriate legal provisions would be highly undesirable.

The Puttaswamy judgment also introduced the doctrine of proportionality with respect to the right to privacy. As observed by the Court, any breach of the right to privacy would need to satisfy the tests of legality, legitimate State aim, necessity, and proportionality. These tenets continue to shape the judicial review of State actions involving privacy right restrictions, and the right to personal data protection.

In the sphere of digital governance and online platforms, the constitutional recognition of the right to privacy of information, particularly from the digital services of a private entity, is of great importance. The State has the duty to protect this information. The protection of the right to privacy of information becomes further pronounced when the digital services of the State itself are used. In this respect, the Supreme Court of India has laid down the legal framework on data protection.

STATUTORY FRAMEWORK GOVERNING DIGITAL PRIVACY IN INDIA

To be in line with new technological advancements and trends in the digital economy, India has updated its legal framework for digital privacy. In the beginning, the Information Technology Act, 2000, established the governing framework for electronic information and

¹³ Maneka Gandhi v. Union of India, AIR 1978 SC 597.

¹⁴ Francis Coralie Mullin v. The Administrator, Union Territory of Delhi, AIR 1981 SC 746.

¹⁵ Justice K. S. Puttaswamy (Retd.) & Anr. V. Union of India & Ors., AIR 2017 SC 4161.

formalized e-commerce and cybercrimes. The Act had some data protection features. For example, Section 43A¹⁶ mandated payment of damages for losing sensitive personal data, and Section 72A provided for a penalty for the wrongful disclosure of personal data.¹⁷

The protection provided in the Information Technology Act, coupled with the 2011 Rules on reasonable security practices, received criticism for their inadequate protection and failure to address the challenges presented by artificial intelligence and cross-border data flow, among others. In response to the above, the Digital Personal Data Protection Act, 2023 (DPDP Act) was passed, and this law was the first in India to address digital personal data protection.

The DPDP Act mandates the protection of personal data be done with the prior consent of data subjects. The Act elaborated the rights of Data Principals and placed certain responsibilities on Data Fiduciaries. In addition, the Act provides for the establishment of the Data Protection Board of India and empowers the Board to grant relief and impose penalties. With the above mentioned features of the Act, the data protection framework in India has been strengthened. Nevertheless, the framework is still deficient in many conflicts.

Critical Analysis of India's Digital Privacy Framework and International Perspective

The Digital Personal Data Protection Act, 2023 marks a watershed moment in India's ability to develop a comprehensive law on data protection. The Act establishes the rights of Data Principals, obligations for Data Fiduciaries, and improves the processing of personal data by establishing the Data Protection Board of India. It improves processing personal data by establishing the Data Protection Board of India.¹⁸ It also addresses the development of constitutional principles in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The development of the right to privacy, where informational privacy is part of the right to privacy, is accommodated. The effectiveness of a law, however, does not rest on its provisions alone. It also depends on the implementation, the enforcement of the law, and the independence of the relevant institutions.¹⁹

One of the major criticisms of the current framework is the broad exemptions that the Digital Personal Data Protection Act, 2023, grants to the State. While some exemptions may be justified in the interest of national security, public order, or the prevention of crimes, the excessive broad discretionary power may dilute the constitutional privacy of the individual.

¹⁶ Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India).

¹⁷ Information Technology Act, 2000, § 72A, No. 21, Acts of Parliament, 2000 (India).

¹⁸ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁹ Justice K. S. Puttaswamy (Retd.) & Anr. V. Union of India & Ors., AIR 2017 SC 4161.

Widespread concerns among legal scholars regarding the balancing of individual rights vis-à-vis the interests of the State, arise from the lack of comprehensive judicial oversight with respect to some of the exemptions. Concerns regarding the independence and functioning of the Data Protection Board also arise from the considerable control exercised by the Central Government over the Data Protection Board. These concerns demonstrate that privacy cannot be effectively legislated without support from transparent institutions and strong mechanisms for accountability.

Protecting people's information is a big problem in practice. Most people who use the internet do not understand the rules about keeping their information private or giving permission for it to be used. They are not aware of their rights under the DPDP Act. Small companies and people who provide services online are likely to have trouble following some of the regulatory rules. So, following the law needs to be helped by teaching people about things, educating the public and making sure the rules are enforced. We need to make sure that people's personal information is handled responsibly. People will not trust the digital world unless there are good systems in place to respond to and protect against data breaches.

Looking at what other countries are doing can help us see where we can improve the rules in India. The GDPR is an established law that protects people's personal information. It has found a balance between protecting people's information and making sure that companies use data responsibly and it includes many important principles like only using the information that is necessary only using it for the reason it was given designing systems that protect information being accountable for what happens to the information and telling people when there has been a big breach of their information. The GDPR also gives people the right to take their information with them when they switch services and the right to have their information deleted. When we compare the DPDP Act to the GDPR we can see that the DPDP Act does not do much to protect peoples' right to take their information with them or have it deleted. It does not have as many independent organizations to oversee the rules and it lets the government make more exceptions.²⁰

²⁰ General Data Protection Regulation (GDPR), No. 679, Acts of Parliament, 2016 (European Union).

FINDINGS

- The Right to Privacy was recognized as a basic right in the landmark judgement of Justice K. S. Puttaswamy (Retd.) v. Union of India (2017).²¹
- The Digital Personal Data Protection Act, 2023 is the first dedicated and complete legislation in the country that aims to provide rights to Indian citizens in the emerging aspect of digital privacy.²²
- Despite the existence of constitutional safeguards, the challenge is regarding the implementation of digital privacy rights as they continue to exist and there exist concerns regarding their enforcement.²³
- The exemptions allowed by the government under the Act creates threats to privacy and individual rights and raises the threat of surveillance.
- The rights are uncertain as to their independence and effectiveness in relation to data protection rights.
- The laws that are now practiced in India do not include any provisions that relate to emerging technologies such as artificial intelligence, facial recognition and deepfake technology. This means that these laws may not provide the protection that data privacy laws require to prevent these technologies from posing threats to people and society as a whole.²⁴
- The comparison between the privacy rights of digital users in India and the privacy protections provided by the European Union's GDPR reveals that while the digital privacy rights of Indian citizens are well-established, there is a need for greater independence in the regulation of these rights, as well as greater transparency and accountability from those who are responsible for enforcing these rights.²⁵
- A multi-dimensional approach is needed to counter the challenges that come to countries in their digital privacy rights. This includes reforms to the legislation of the country, strong institutional bodies to enforce those laws, better cyber security

²¹ Justice K. S. Puttaswamy (Retd.) & Anr. V. Union of India & Ors., AIR 2017 SC 4161.

²² Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

²³ Charru Malhotra, *Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India*, 70 Sage Journals. 516, 531 (2024) <https://journals.sagepub.com/doi/10.1177/00195561241271575>. (last visited Jul. 5, 2026)

²⁴ Abhinav Singh, *Automated Profiling, Privacy Rights, and Gaps in India's DPDP Act 2023*, 9 IRE Journals. 3521, 3527 (2026) <https://www.irejournals.com/paper-details/1717032>. (last visited Jul. 5, 2026)

²⁵ General Data Protection Regulation (GDPR), No. 679, Acts of Parliament, 2016 (European Union).

infrastructures to protect the digital information of people, enhancing the digital literacy of the citizens of the country, an accountable government and a review of those laws and their implementation. Also, initiatives should be taken to raise awareness of these rights among the citizens of the country through campaigns and advertisements.

In general, the digital privacy structure of India has shown important growth in safeguarding the personal data of its people. However, its success in the long run will depend on the implementation of these rights, continued research in the field, public awareness of these rights and transparency by the government and institutions of India in implementing these rights.

CONCLUSION

The growth of digital technology has significantly changed how we communicate, access services, conduct transactions, and use many other electronic technologies. Digitalization has brought huge benefits in economic development and inventions. But, as a result, the amount of data collected, processed, and saved has tremendously increased which makes respect for people's digital privacy a very important legal and constitutional issue. This project has a goal to analyze digital privacy aspects in India from the point of view of constitutional recognition of the right to privacy,²⁶ legal provisions offered by the IT Act of 2000²⁷ and the Digital Personal Data Protection Act of 2023, and practical issues of personal data protection.²⁸

The results show that the recognition of the right to privacy as a fundamental right in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) has become a turning point in the development of the Indian constitution.²⁹ The passing of the Digital Personal Data Protection Act of 2023 has made the legal basis for digital information protection even stronger granting rights to people and responsibilities to organizations dealing with digital information. At the same time, the findings suggest that the presence of laws on the paper does not ensure great privacy protection. Implementation of various problems such as the lack of supervision,

²⁶ INDIA CONST. art. 21.

²⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

²⁸ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

²⁹ K. S. Puttaswamy (Retd.) & Anr. V. Union of India & Ors., AIR 2017 SC 4161.

government exemptions, digital education and cyber security contribute to the problems arising during enforcement of the right to privacy.

To sum up, Indian digital privacy laws have marked progress toward protecting citizens in the digital environment. However, their success will rely on how well the government implements them and cooperates with the stakeholders. A compromise between innovation and preservation of people's constitutional rights suggests creating a safe digital environment.