

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.  
All rights reserved.**

## ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

## ***PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT***

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

# **RIGHT TO PRIVACY AFTER K.S. PUTTASWAMY V. UNION OF INDIA: MYTH VS REALITY**

AUTHORED BY - MOHIT KUMAR

B.A.LL.B., NMIMS Kirit P. Mehta School of Law, Mumbai

## **1. ABSTRACT**

The judgment of the Supreme Court in *K.S. Puttaswamy v. Union of India* declaring privacy as a Fundamental Right of the citizen under Article 21 of the Constitution proved to be a turning point in the history of Indian constitutional jurisprudence. In this case, privacy was considered a fundamental part of human dignity and an essential facet of life and liberty that should be respected at all costs. The apex court had also provided for certain criteria like legality, necessity, and proportionality to be used for examining any encroachment by the State on this right of privacy. However despite its recognition as a Constitutional Right, the implementation of the Right to Privacy in India continues to be problematic. This paper discusses whether there exists a disconnect between theory and practice when it comes to privacy rights in India. The research seeks to examine the inadequacy of current measures towards ensuring the protection of the Right to Privacy in India in the face of increasing state surveillance and weak safeguards. The paper further evaluates the efficacy of the Digital Personal Data Protection Act, 2023 in guaranteeing protection against misuse of personal data in India.

## **2. KEYWORDS**

Right to Privacy; Article 21; *K.S. Puttaswamy v. Union of India*; Constitutional Law; State Surveillance; Data Protection; Digital Personal Data Protection Act, 2023; Informational Privacy; Proportionality; General Data Protection Regulation

## **3. INTRODUCTION**

The fast-paced development of new technologies and the governance of data has led to fundamental changes in the relationship between individuals and the State, making privacy the key issue of constitutional importance in many jurisdictions. With respect to India, *K.S. Puttaswamy v. Union of India*<sup>1</sup> case was the milestone in the history of the development of the

---

<sup>1</sup> *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

constitutional law in this country, where the Supreme Court unanimously ruled that the right to privacy is an intrinsic part of life and liberty guaranteed by Article 21 of the Constitution<sup>2</sup>. The Court not only rejected all previously accepted positions regarding the non-existence of a fundamental right to privacy<sup>3</sup>, but also developed a system of criteria for assessing the intervention into people's rights based on the notions of legality, necessity, and proportionality<sup>4</sup>. In this way, the Court created a new legal framework in India concerning the right to privacy in the age of increasing digitalization and the massive accumulation of data.

However, although there exists such constitutional protection, the question arises if privacy in India is actually protected. With the increasing surveillance methods and biometrics in India, as well as the development of data governance, it becomes necessary to ask about the actual enforcement of the right to privacy. Moreover, recent developments in legislation, like the introduction of the Digital Personal Data Protection Act, 2023<sup>5</sup>, may be considered a step forward but still suffer from certain flaws, namely wide exceptions granted to the State and weak enforcement mechanisms. The goal of this paper is to critically analyse the difference between constitutional promises and the actual reality of privacy protection. The purpose of the analysis will be to understand whether the recognition of privacy as a constitutional right has resulted in effective protection or remained merely symbolic. Through an examination of legal developments, case law, and other sources, like the GDPR, the author will attempt to prove that although privacy in India is undoubtedly guaranteed, its implementation faces numerous obstacles.

#### 4. EVOLUTION AND RECOGNITION OF PRIVACY

The right to privacy in India has developed gradually through judicial interpretations, and is not enshrined in the Constitution of India<sup>6</sup>. For instance, during its early days, the Supreme Court of India did not view privacy as a fundamental right<sup>7</sup>, and interpreted personal liberty from a limited perspective. In recent times, however, there has been a major reinterpretation of Article 21 of the Indian constitution<sup>8</sup>, which stipulates that everyone has the right to live with dignity, and personal liberty. In other words, the Supreme Court realized that the right to life

---

<sup>2</sup> Constitution of India, Article 21.

<sup>3</sup> *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300; *Kharak Singh v. State of UP*, AIR 1963 SC 1295.

<sup>4</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>5</sup> Digital Personal Data Protection Act, 2023.

<sup>6</sup> Constitution of India.

<sup>7</sup> *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300; *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

<sup>8</sup> Constitution of India, Article 21.

and personal liberty covers many different factors that make living with dignity possible.

However, the issue was conclusively resolved in *K.S. Puttaswamy v. Union of India* (2017)<sup>9</sup>. In this case, a nine-judge bench of the Supreme Court held, unanimously, that the right to privacy is an integral part of Article 21. In this case, the Court stated that the right to privacy is inherent in human dignity, freedom, and individuality. Privacy is made up of many components, including, but not limited to, personal autonomy, bodily integrity, and informational privacy. Further, the Court laid out guidelines regarding how the government can regulate the privacy of citizens. Any interference in privacy must fulfill certain requirements to qualify as valid. Firstly, it should be backed by law; secondly, there should be a legitimate purpose for the intervention; and thirdly, the intrusion must be proportional to the aim it seeks to achieve<sup>10</sup>. Therefore, the recognition of privacy as a fundamental right has been a defining moment in Indian constitutional law history. It has been established as a key element of a democratic polity and will be crucial in handling new challenges arising from the modern world.

## 5. SCOPE OF PRIVACY RIGHTS

Privacy in India is a complex and developing idea that extends beyond physical privacy. Once privacy was acknowledged as a basic right<sup>11</sup>, it became multi-faceted and necessary for safeguarding individual dignity and autonomy. Privacy encompasses many dimensions of an individual's life rather than focusing on just one aspect. One such dimension is informational privacy<sup>12</sup>, which is aimed at protecting individuals' personal information and providing them with control over their own information. Similarly, another facet of privacy is bodily privacy, which involves protecting a person from any kind of invasion into his or her body. Moreover, decisional autonomy gives individuals freedom to make personal decisions about marriage and family matters.

But the Right to Privacy is not an absolute right. The State has the power to regulate the right provided that there is a law, proper purpose, and proportionality involved. As a result, the sphere of the Right to Privacy in India is very broad, and it continues to widen, particularly with the advancements in technology and the increasing significance of safeguarding one's personal

<sup>9</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>10</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>11</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>12</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

information.

## 6. MYTH VS REALITY OF PRIVACY

The acknowledgment of privacy as a fundamental right<sup>13</sup> led to the creation of a myth that privacy is protected in India. It is based on the idea that once recognized as a fundamental right, privacy will be sufficiently protected in its aspects related to personal data and dignity. People tend to think that they can control all the aspects related to the use of their personal data, and any violations will be prevented because the State cannot interfere in people's lives and violate their rights arbitrarily. In fact, it seems that with the help of this ruling, the legal system ensured the protection of people's privacy rights.

Still, the reality is quite opposite to what many people tend to think today. Although privacy is recognized in the Constitution<sup>14</sup> of the country, privacy laws in India remain rather ineffective due to increased surveillance, extensive collection of data, and failure of authorities to enforce existing laws. In fact, despite the fact that the laws exist, there are some general exclusions that allow to use private data in certain situations. Moreover, people do not always control the use of their personal information, and consent is not always voluntary and sincere.

## 7. PRIVACY CHALLENGES IN INDIA

The privacy laws in India are currently under threat as a result of the increasing use of various surveillance devices by the State<sup>15</sup>. With technological advancements such as biometrics, facial recognition and other forms of digital surveillance becoming popular, there has been increasing use of such technologies in the name of national security, public safety and administrative efficiency. While the use of these technologies may be seen as justified based on considerations such as national security and public safety, there have been concerns about their impact on privacy. There are no legal limitations on how these surveillance devices can be used; therefore, it has become easy for any individual to abuse the system through invasion of the privacy of others. Additionally, since people do not know what surveillance methods are employed by the State, they are unable to manage their privacy.

Yet another significant problem is the lack of effective enforcement of privacy rights. Privacy

---

<sup>13</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>14</sup> Constitution of India, Article 21.

<sup>15</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

has been established as a basic right<sup>16</sup>, but the instruments that have been provided to implement it do not suffice. There is much ambiguity in various existing legal measures like those regarding data protection<sup>17</sup> because of many wide-ranging exceptions, especially in favour of the State. Moreover, there are no adequate bodies to oversee the observance of any privacy norms. Consent, which plays an important role in the matter of privacy, becomes an issue due to the willingness of people to share personal data despite lacking adequate information about what might follow. Judicial delay and inconsistency further exacerbate the problem of enforcing privacy rights.

## 8. DATA PROTECTION AND LEGAL FRAMEWORK

Data protection has come to be an important element of privacy within the Indian context<sup>18</sup>, given the rise in digitalization and data-based governance. As a result of the increase in the usage of online platforms, digital services, and various databases, a large number of individuals' personal information can now be accessed and stored. Such a reality highlights the importance of enacting laws for ensuring a reliable level of data protection. However, despite having declared privacy as one of the fundamental rights in the Constitution of India, the lack of a proper and efficient data protection regime has been a problem until very recently.

To address the issue, the Indian government enacted the Digital Personal Data Protection Act, 2023<sup>19</sup>. The legislation introduces a framework of regulations for the collection and use of personal data within the country. According to the act, data fiduciaries have certain obligations and duties when processing data. Additionally, data principals, or the affected individuals, have several rights in regards to their information. Importantly, the act emphasizes the obligation to process personal data lawfully, with the individual's consent and in pursuit of certain specified purposes<sup>20</sup>.

However, despite its importance, there are several criticisms regarding the Act. Among them, the most notable one is the existence of broad exemptions provided to the State regarding issues involving national security, public order, and sovereignty. Such exemptions mean that government entities can evade some of the protections provided in the law, thus reducing the

---

<sup>16</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>17</sup> Digital Personal Data Protection Act, 2023.

<sup>18</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>19</sup> Digital Personal Data Protection Act, 2023.

<sup>20</sup> Digital Personal Data Protection Act, 2023.

overall legal safeguards. Moreover, there is controversy surrounding the efficacy of the enforcement process provided under the Act, where the success of the regulatory body relies much on the operational capacity of the Data Protection Board<sup>21</sup>. From the legal point of view, it can be said that Indian courts have made significant contributions in terms of framing data protection and privacy issues<sup>22</sup>. After establishing privacy as a fundamental right, the emphasis has been laid on balancing individual rights with the concerns of the State. It should also be noted that the use of privacy principles in individual cases has not always been consistent, thus causing some problems in implementation. Even though the courts have taken the issue of informational privacy into account, its modern aspects have yet to be addressed properly.

Also, the notion of consent, which is at the heart of data protection legislation, poses some problems when put into practice. Citizens do not have a clear idea of the risks involved with having their personal information collected and processed and as such give consent in a somewhat superficial manner. Such consent does not help to meet the objective of protecting personal autonomy. Additionally, there seems to be a lack of knowledge on the part of citizens concerning their data rights. Therefore, even though India has made strides in formulating its data protection regulations both legally and judicially, there still exists room for improvement in this matter. The current framework represents a certain level of advancement in terms of the realization of informational privacy rights, but its effectiveness is affected negatively by numerous exemptions and the weaknesses present in the mechanism for enforcing data protection rules.

## 9. COMPARATIVE ANALYSIS

The comparison between the data protection policies in India and international standards shows considerable differences regarding their scope and implementation. The General Data Protection Regulation<sup>23</sup> is one of the best data protection laws worldwide. This regulation covers data protection within the European Union and features a robust legal framework. Individual rights are the core principles of the regulation, alongside the accountability of data controllers and strict regulatory control. Thus, the GDPR is often considered an exemplary framework for data protection policies throughout the globe. First, it should be noted that the rights of individuals vary greatly in the GDPR and the Digital Personal Data Protection Act,

<sup>21</sup> Digital Personal Data Protection Act, 2023.

<sup>22</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>23</sup> General Data Protection Regulation (EU) 2016/679.

2023<sup>24</sup>. The GDPR guarantees individuals numerous rights, including access, rectification, erasure (or "right to be forgotten"), and restriction or objection to data processing. Individuals can benefit from these rights in cases when their personal data is processed. However, India's Digital Personal Data Protection Act, 2023 only provides some basic individual rights concerning data processing, including the right to obtain data, correction, and removal. Additionally, individuals have the right to withdraw consent for the further use of their data in accordance with the act. Still, their rights are rather restricted under this regulation.

The second major difference pertains to enforcement procedures. According to the GDPR, there are independent supervisory authorities in all member states tasked with monitoring compliance and enforcing data protection provisions. These authorities are vested with wide ranging powers, among them the ability to levy massive fines on entities failing to comply with the provisions of the Act<sup>25</sup>. Strict punitive measures under the GDPR effectively serve as a disincentive to abuse. By comparison, India's scheme makes use of the Data Protection Board whose effectiveness is questionable<sup>26</sup>. The lack of an independent enforcement mechanism makes the enforcement process weak in India. A third difference is found in the matter of exemptions for the State. In accordance with the GDPR, even State activities will be subject to restrictions and oversight. This provision seeks to guarantee that individual privacy is not compromised by governmental bodies without justification. On the other hand, India's Act grants State-wide exemptions on grounds of national security, public order and public health<sup>27</sup>. Informed consent and transparency of the processes have differences in both approaches as well. The GDPR requires explicit consent, meaning individuals should be explicitly told why their data is being collected and how it will be used by the company. They must be adequately informed about all the procedures in order to provide their informed consent. In India, the issue of consent is significant as it forms part of the Indian data protection laws, but individuals may only provide consent formally or superficially without realizing fully the consequences. Therefore despite the development of a data protection law by India, there is still much that needs improvement in the legal structure concerning the requirements of GDPR. In particular, stronger mechanisms must be enforced; exemptions made by the States should be minimized; and rights of the individuals need to be better protected. The process will require learning from the best practices abroad.

---

<sup>24</sup> Digital Personal Data Protection Act, 2023.

<sup>25</sup> General Data Protection Regulation (EU) 2016/679.

<sup>26</sup> Digital Personal Data Protection Act, 2023.

<sup>27</sup> Digital Personal Data Protection Act, 2023.

## 10.REFORMS AND RECOMMENDATIONS

To make the right to privacy a meaningful one in the Indian context, it becomes imperative to amend the existing laws and institutions to provide greater efficacy to this right<sup>28</sup>. An important reform in this regard would involve the provision of concrete restrictions on state surveillance activities. Though surveillance activities by the state are often necessary in the interest of national security, there is a need for clear legislative provisions that define the boundaries, process, and procedures involved in such surveillance activities. A second key reform involves amending the existing Digital Personal Data Protection Act of 2023<sup>29</sup> to make the provisions stronger in terms of data privacy laws. The law needs to be amended so as to minimize exemptions that have been granted to the State as a result of which the law has become largely meaningless when it comes to protecting the right to privacy. It must be ensured that while the interests of the state are safeguarded, there is no infringement of individual liberties.

An independent regulatory agency is also required for proper enforcement of the law. The enforcement capacity of such laws depends to a great extent upon the efficiency and independence of the agency responsible for enforcing it. The Data Protection Board would need to have greater independence and autonomy so that it can fulfill its responsibilities<sup>30</sup>. In addition, adequate financial and human resources are required to achieve these ends. Moreover, there should be a focus on increasing awareness among citizens regarding their privacy and data rights. They need to be made aware of their data rights and consequences of giving personal data. Informed consent is an important element that requires further improvement to make sure that data subjects give their consent freely and without coercion and know what the data controller plans to do with their data. Another measure which can be adopted to strengthen privacy rights is the use of judiciary. The courts need to adopt a positive attitude towards this issue and use their powers as prescribed by the constitution and its jurisprudence. There is also a need to develop a judicial precedent in dealing with modern day privacy concerns such as data breach and surveillance activities.

Moreover, India can learn a lot through the adoption of global best practices, including the adoption of the General Data Protection Regulation<sup>31</sup>. This includes elements like enhanced

---

<sup>28</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>29</sup> Digital Personal Data Protection Act, 2023.

<sup>30</sup> Digital Personal Data Protection Act, 2023.

<sup>31</sup> General Data Protection Regulation (EU) 2016/679

individual rights, severe penalties, and independent oversight in improving the overall efficiency of India's data protection laws. Comparative law can be useful in bridging gaps and helping India harmonize its laws with other international laws.

Finally, there is a need to ensure continued review and modification of privacy laws. With technology continuing to advance in areas like artificial intelligence, big data analytics, and digital surveillance, the legal framework has to be adaptable. Modifications and policy updates in this regard will ensure the laws are effective and responsive. In conclusion, India has made significant progress towards recognition and regulation of the right to privacy. However, important changes and reforms are needed to bridge gaps between the right in theory and in practice. Enhanced legal protections, effective enforcement measures, and public education on the matter will go a long way in promoting the right to privacy in today's digital age.

## 11.CONCLUSION

The recognition of the right to privacy as a fundamental right in India constitutes one of the most important landmarks in constitutional law jurisprudence. This is because of the progressive recognition of the concepts of dignity, autonomy, and liberty. Moreover, the acknowledgment of privacy as being an integral part of the right to life and personal liberty constitutes another step forward towards ensuring that individuals can protect themselves from any form of State interference especially in times when there has been tremendous development in technology and digitization of society .Despite this recognition as a fundamental right, there still exist many problems in relation to the implementation of privacy as a right. This is evident from the discussion of various issues in this paper. These include the increased scope of State surveillance as well as data collection and storage without clear legal limits among others. All these are justified in terms of national security and administration, yet their execution presents many risks to individual liberty.

The introduction of the Digital Personal Data Protection Act, 2023 represents an important development for the establishment of data protection legislation in India. However, even if the Act provides for various rights and obligations, its effectiveness is hampered by the existence of large state exemptions, lack of efficient enforcement tools, and doubts about the independence of authorities. By drawing a comparison with international acts, including the General Data Protection Regulation, it becomes clear that there is a need to improve this situation. Thus, despite having achieved much success in the recognition and development of

the right to privacy in the country, further reforms are needed to make sure that its realization is ensured. It is necessary to develop effective laws, reduce State interference, introduce appropriate enforcement procedures, and raise the level of awareness among people. Ultimately, the right to privacy needs to be more than just a constitutional right and become a reality in practice.

## BIBLIOGRAPHY

### A. Cases

- *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
- *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300
- *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295
- *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148
- *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632

### B. Statutes

- Constitution of India
- Digital Personal Data Protection Act, 2023
- General Data Protection Regulation (EU) 2016/679

### C. Books

- M.P. Jain, *Indian Constitutional Law*
- V.N. Shukla, *Constitution of India*

### D. Articles and Journals

- Research articles on right to privacy and data protection in India
- Scholarly writings on digital privacy and surveillance
- Comparative studies on GDPR and Indian data protection laws

### E. Reports and Online Sources

- Government reports on data protection and privacy
- Articles on surveillance and privacy issues in India
- Legal databases such as SCC Online and Manupatra