

INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

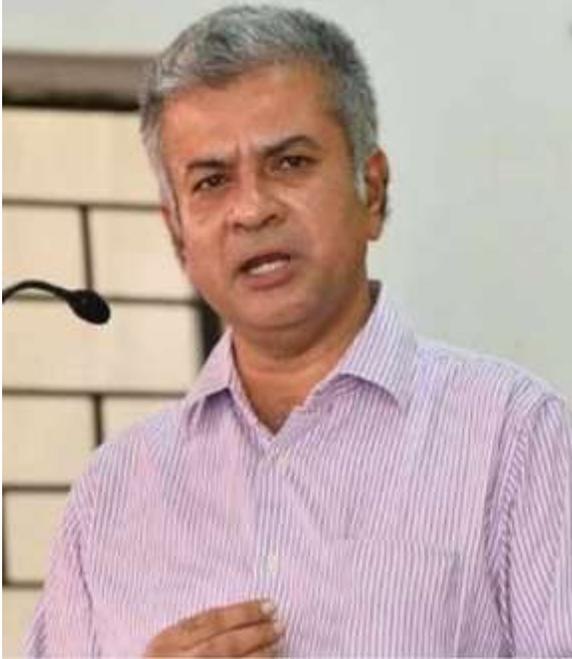
No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

– The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a

professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of Law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.



Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provided dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

RIGHT TO PRIVACY IN INDIA

AUTHORED BY - SHEETAL SHARMA & SALTANAT SHERWANI

ABSTRACT

The Indian privacy concept has clearly turned the table within a short span of time. Though not directly referred to in the constitution but it has been respected as a fundamental right which flows from article '21 of the constitution that provides the right to live and personal liberties. It covers the preceding article which discusses privacy rights initiation in India from the pillar judgement Justice K.S. Puttaswamy (Retd). and vs. Union of India (2017). This case enhanced the right to privacy and classified it as a principle right with needs for diligent restrictions for the best interest of public safety and security.

This article subsequently expounds the legal structure regarding privacy rights in India. This incorporates the Information Technology Act, 2000, which comes together with data security and privacy conditions. More importantly, we will focus our attention on the Digital Personal Data Protection Act (DPDP) Act, 2023, to evaluate its possible implications on the right to privacy. This article looks into the objectives of DPDP Act and how it provides individuals with an enhanced level of power over their personal data and how it is in line with developed precepts from the Puttaswamy Case.

Although progress in this regard has been quite considerable, the article does admit that there still are aspects that require further attention and thus make it quite difficult to ensure strong privacy protection. Its focus is on state-run wiretapping or monitoring networks which pose problems to human rights in terms of privacy and the DPDP Act. The abstract summarizes by mentioning the ever-need of consistent updating of the legal landscape. This comprises of demanding legislative reform suggestions so that the fundamental framework can be created that harbors the harmonious existence of the personal private rights and the state legitimacy interests in the digital era that keeps changing.

KEYWORDS: *Indian privacy concept, Constitution, Right to privacy, Justice K.S. Puttaswamy (Retd). and vs. Union of India (2017), Digital Personal Data Protection Act (DPDP) Act, 2023, Data security, Legislative reform.*

INTRODUCTION

Think of how easily your life might be revealed online, with each sale, search or social network interaction being thoroughly recorded and searched. It's not something from a sci-fi movie, but it is the truth that we live in the information age. The need to protect one's privacy has been on the rise as we are going through the world where digital interactions are much more prevalent. Nevertheless, the question that arises is what the content of this right is in India? The right to privacy for individual in the Indian context is beyond locking your diaries and private letters. It's about ensuring the protection of an increasingly essential component of your identity in the online world. It means the right to know what information about you is being collected, how it is being used, and with whom it is being shared. Through this information creation, you depict yourself and your activities, even your ideas in a broad digital footprint.

The right to the privacy of your image is yours to choose who gets to see it. You have the power to disclose same details to some trusted communities and let that secrets remain unknown to people who can use them wrongly. This very trait empowers the individual in the digital world, shields their sense of autonomy from the feeling of being reduced to a single data point in a monster machine.

Nonetheless, the constitutional protection of privacy in India doesn't go back long enough. In contrast to a few Western countries, India's ascent towards an impenetrable data privacy system has been a very gradual and constant process. Before the Constitution was interpreted, the right to privacy was not spelled out in it as a basic right. However, the watershed moment arrived in 2017 when, somehow, everything changed.

In the *Puttaswamy v. Union of India* case, during 2017, the Supreme Court of India declared privacy as a fundamental right which falls under the scope of Article 21 in the Constitution. The Constitution takes into account such virtues by securing that an individual's right to life and liberty is certainly not violated. Extending the Liberty Concept, the Court's judgement extended the idea to also include a new kind liberty – informational privacy which refers to the right to control what the collection, use and disclosure of your personal information.

As the essence of personal data protection goes beyond mere confidentiality. It encompasses various aspects of your life, including:

- **Bodily Privacy:** The bodily autonomy and the ability to take your own decisions about your health without anyone interfering in your life.
- **Informational Privacy:** Let me elaborate, on the right to control your personal information, which is another important consideration.
- **Decisional Privacy:** The guarantee of the freedom to take one's own decisions and without any imposition.

This right of the privacy also plays the role of the shield, which protect all of your aspects such as the feeling of self, the financial safety, and the physical safety during the digital realm. We will further elucidate the repercussion of Puttaswamy judgment and discuss how this judgment brought data privacy to the forefront in the Indian legal landscape in the upcoming section of this article.

Puttaswamy v. Union of India (2017 Judgement: Recognizing Privacy as Fundamental Right)

The game changer is the Puttaswamy judgment which has made a fictional fiction by declaring that the right to privacy is a fundamental right indeed that is quite consequential when it comes to the search and seizure powers. The Gobind case that involved the acknowledgment of limited privacy rights and the quotation of the personal space like home as mainly protected from privacy invasion, was the only available privacy law in the country before this landmark ruling. Instead, he drafted a similar law in that any law that infringes on the right to privacy must pass the test for the compelling state interest. Nevertheless, these judgments also contributed meaningfully to this dynamic such as the later judgments PUCL and Canara Bank. For an example, Crimea Bank maintained that wherever an individual possesses a certain level of privacy, the other side of his/her property should be considered private too. This bank introduced the "reasonable expectation of privacy" test in order to limit impressive search powers.

However, the evolution took another path in the Puttaswamy (2) v. Union of India case, commonly known as the Aadhar case. On this account, the court, while the court imposed a hard test for assessing the adequate manner of compensating the infringement of privacy measures, proved itself as subsidiary to the state. However, most of them were more thoughtful about the wording of the law rather than its live operation. Such dissatisfaction bothered many people. Instead, Justice Chandrachud's opinion delivered the dissenting view and attempted to encroach on state's interest by using a tougher scrutiny standard at the expense of proportionality. He was inspired by the communicative state interest test's robustness, urging for a stricter approach to the process. Create

your own visitors account and benefit from exclusive services, including free lessons, downloads, discounts, and more.

Basically, this judgment to some extent redefined the concept of privacy and their components as fundamental rights and makes the search and seizure provisions subjected to a more accurate judicial prisme. While the landmark cases like Gobind preceded it, the cases such as did practically apply it to the real world. Nevertheless, the aforementioned case showed disagreement between the law that the court set out and what the court scrutinized more as on this point the majority of judges threw their weight behind the government.

- **Connection between Right to Privacy and Data Ownership/Control**

Try to place yourself in shoes of such organisations whose secrets are exposed. Imagine your personal information – your name, address and health records being resolutely collected and analyzed by companies and organizations. This is not a fictional future with all its nightmares; it's the mirror of the digital world we have today. In this digital society, the right to privacy is also a must, and this is what can give you the chance to own and to not share your personal data – your data ownership. The Right to Privacy: For instance, the Foundation sets the rules for implementing state level reforms and classifies political parties as either interested in change or reluctant to change. The Privacy of the citizen, a fundamental right as declared in India in 2017 in the Puttaswamy judgment, assists people in managing their information. This holding of keys goes beyond just protecting your private diaries or your personal correspondence. It encompasses the ability to:

- i. **Decide who collects your data:** You have the right to say no or grant your consent to the data collection of different physical and digital entities.
- ii. **Determine the purpose of data collection:** Organizations cannot collect your data without your consent and must set a goal and define the mechanism via which they intend to use it.
- iii. **Control how your data is used:** You are entitled to set the rules for what you want to do with your data and how it should not be used beyond the scope of your authorized consent.
- iv. **Access and rectify your data:** It is your right to ask for access to the data stored about you by any organization and correct any errors in your personal data.
- v. **Erase your data:** The removal of personal information depends on whether you meet some special circumstances and ask for such an action.

This control of your data makes you feel independent in the digital environment, a dependence

that is present on everything is gone. It keeps you from having a creeping feeling like you're just a number in a huge system. Eventually, it gives you the control to make considered choices on how you appear online.

Data Ownership in Action: The said Act of DPDP. India's all-new Digital Personal Data Protection Act (DPDP) of 2023 built on the already existing principles from the Puttaswamy judgement. The DPDP Act establishes clear guidelines for data fiduciaries (organizations collecting and processing personal data) regarding:

- i. **Consent Requirements:** Companies have to ask for the permission and approval of individuals before gather their private information.
- ii. **Data Minimization:** The personal data collected by data fiduciaries are only for the specific use to which it has been limited.
- iii. **Data Security Measures:** Security procedures should be strengthened and data should not be accessed by unauthorized individuals or used in an unethical way.
- iv. **Individual Rights:** The Information Privacy Act stipulates that individuals have the right to access, rectify, and delete their personal data.

The DPDP Act in conjunction with the right to privacy create a framework in India for the ethical use of the pertinent data. This framework underlines that each person has right to participate in the process of collecting, using and storing their data. Therefore, the digital environment becomes not only fair but also more balanced.

- **Privacy a Multifaceted Approach**

It mostly meant the right to have your own space and other private belongings under your control. Puttaswamy judgment, though, broadened the definition of privacy to digital space. This right to privacy empowers you to control your personal information in several crucial ways:

- i. **The Power to Choose¹:** You are empowered to find out which organizations can collect your personal information. You are no longer obliged to provide your data as a prerequisite to enjoy online services.

¹ (Schwartz, P. M. (2017). *Democracy and legal theory*. Cambridge University Press.) as accessed on 19.03.2024

- ii. **Transparency and Purpose²:** No data collection is possible without your informed permission. There should be an obvious declaration on the purpose of data collection which is supposed to serve the specified goal without being misused or abused.
- iii. **Controlling Your Digital Footprint³:** You have a right to restrict how your information is used. This makes it impossible to sell or share the data for purposes beyond that of your initial consent.
- iv. **Seeing and Correcting⁴:** You can request access to your personal data where organizations hold it. This gives you the chance to confirm the exactness of the provided information and if it correctly portrays your identity.
- v. **The Right to be Forgotten⁵:** In some cases, organizations can be asked to erase your personal data from their system on your demand. This way you will be in control of your online presence as well as the consequences from any mistakes or information you might not want to be seen.

Autonomy in the Digital Age & Road ahead

⁶This control over your data fosters a sense of autonomy in the digital age. Imagine navigating a bustling marketplace where vendors constantly track your movements and preferences. The right to privacy empowers you to say "no" to data collection, preventing you from feeling like a mere product or statistic in a vast ocean of information. It allows you to make informed choices about your online presence, shaping how you interact with the digital world.

The Puttaswamy judgement has laid the foundation for a more balanced digital ecosystem in India.

² (Ohm, H. (2010). *Privacy in the age of Big Data: Stumbling towards a new deal*. Stanford Law Review, 65(1), 277-314.) as accessed on 19.03.2024

³ (Solove, D. J. (2004). *Understanding privacy*. Oxford University Press.) accessed on 19.03.2024

⁴ (Nissenbaum, H. (2010). *Privacy in a technological world*. Cambridge University Press.)

"Data Protection Laws in India: Their Evolution and Analysis" by A.K. Legal & Associates (2023): This paper provides a legal analysis of the evolution of data privacy laws in India, examining how different legislations like the IT Act and the Aadhaar Act contribute to the overall framework. This might be on the law firm's website, so availability may vary: <https://sflc.in/ready-reckoner-on-data-protection-in-india-a-comparative-legal-analysis/>

⁵ (European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (accessed on 19.03.2024

11 The Personal Data Protection Regulation (Regulation 2016/679, in English General Data Protection Regulation, abbreviated GDPR)

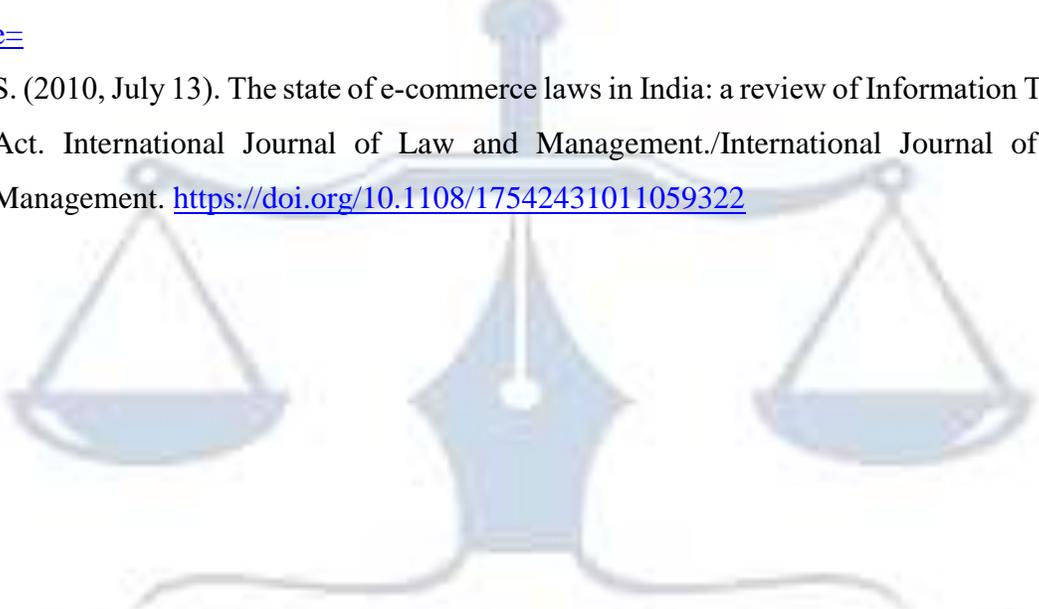
"An Analysis on Data Protection in India" by Indian Journal of Integrated Research in Law (IJIRL) (2022): This paper delves into the landmark Puttaswamy judgment and its impact on recognizing the right to privacy as a fundamental right in India. It also discusses the proposed PDPB and its potential role in data protection. Limited preview might be available on the journal's website, subscription may be required: <https://ijirl.com/wp-content/uploads/2022/03/AN-ANALYSIS-ON-DATA-PROTECTION-IN-INDIA.pdf>

As technology continues to evolve, ongoing discussions and legal refinements will be necessary to ensure that individuals retain control of their personal information. By recognizing the right to privacy as a cornerstone of individual liberty, India has taken a critical step towards a future where individuals, not corporations, hold the keys to their digital selves.

REFERENCES

1. Kumaraguru, P., & Cranor, L. F. (2006, January 1). *Privacy in India: Attitudes and Awareness*. Lecture Notes in Computer Science. https://doi.org/10.1007/11767831_16
2. *About - Hein Online*. (2024, April 3). HeinOnline. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/indiajoula6&div=6&id=&page=>
3. Privacy and data protection in India on JSTOR. (n.d.). www.jstor.org. <https://www.jstor.org/stable/26441284>
4. The Four Parts of Privacy in India on JSTOR. (n.d.). www.jstor.org. <https://www.jstor.org/stable/24482489>
5. Kumaraguru, P., & Sachdeva, N. (2012, January 1). *Privacy in India: Attitudes and Awareness V 2.0*. Social Science Research Network. <https://doi.org/10.2139/ssrn.2188749>
6. Tripathi, S., & Tripathi, A. (2010, September 7). *Privacy in libraries: the perspective from India*. Library Review. <https://doi.org/10.1108/00242531011073146>
7. *About - HeinOnline*. (2024, April 3). HeinOnline. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/ijlj11&div=48&id=&page=>
8. Subramanian, R. (2009, March 15). *Security, Privacy and Politics in India: A Historical Review*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2186523
9. Agarwal, A. & HCL Infosystems. (2020). *SANCTITY OF PERSONAL DATA: a COMPARATIVE STUDY OF DATA PRIVACY LAWS IN EU, US AND INDIA*. In *INTERNATIONAL JOURNAL OF LEGAL DEVELOPMENTS AND ALLIED ISSUES* (Vol. 6, Issue 3) [Journal-article]. <https://observatoriogpd.com/wp-content/uploads/2020/06/Anisha-IJLDAI.pdf>

10. Ahmad, N. (2009, January 1). Restrictions on cryptography in India – A case study of encryption and privacy. Computer Law and Security Report/Computer Law & Security Report. <https://doi.org/10.1016/j.clsr.2009.02.001>
11. Srinivasan, J., Bailur, S., Schoemaker, E., & Seshagiri, S. (2018, March 1). Privacy at the Margins| The Poverty of Privacy: Understanding Privacy Trade-Offs From Identity Infrastructure Users in India. Srinivasan | International Journal of Communication. <https://ijoc.org/index.php/ijoc/article/view/7046>
12. About - HeinOnline. (2024, April 3). HeinOnline. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nlsind26&div=16&id=&page=>
13. S. (2010, July 13). The state of e-commerce laws in India: a review of Information Technology Act. International Journal of Law and Management./International Journal of Law and Management. <https://doi.org/10.1108/17542431011059322>



WHITE BLACK
LEGAL