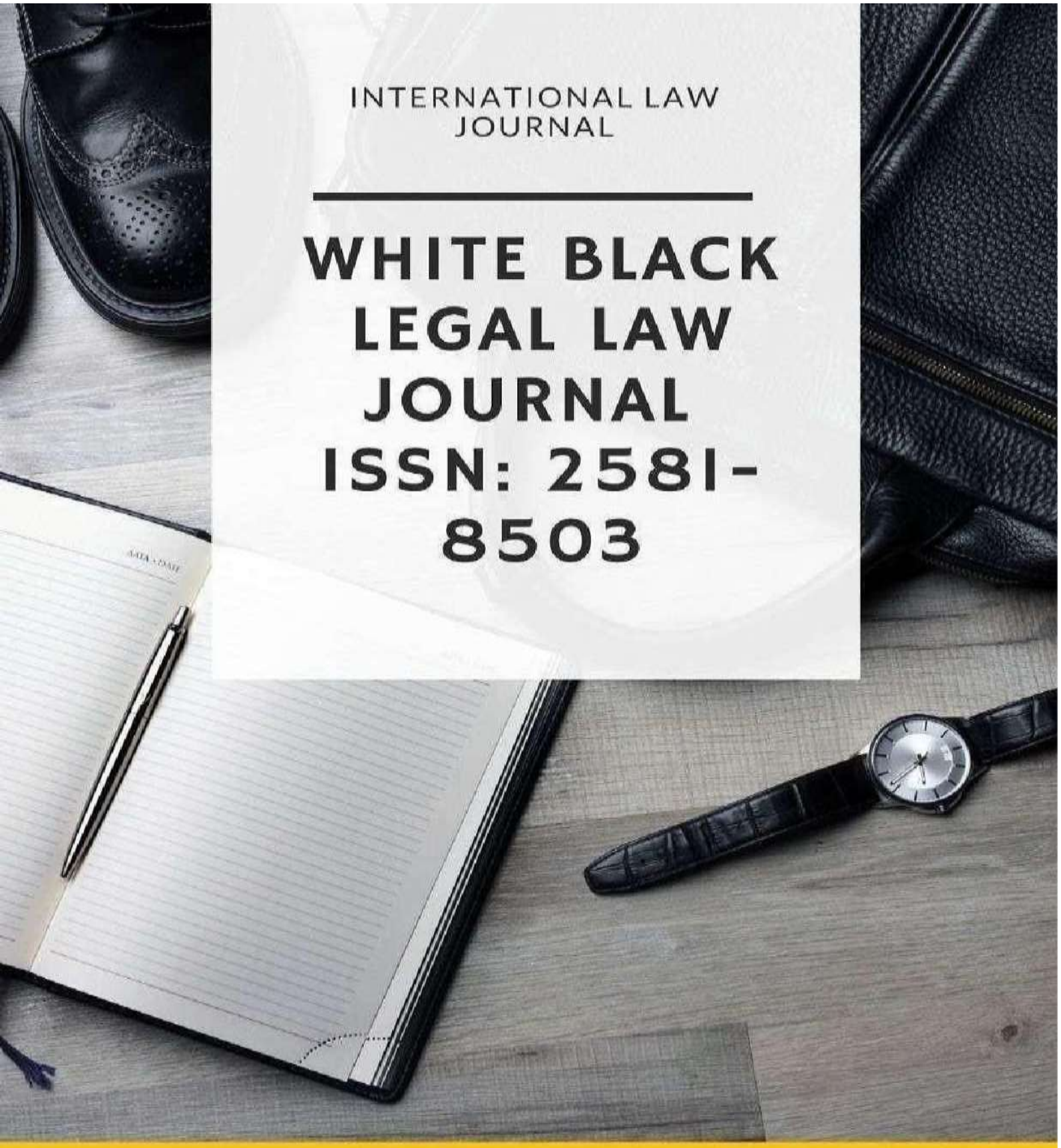

INTERNATIONAL LAW JOURNAL

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, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

INDIA'S PRIVACY TURN: CONSTITUTIONAL PROPORTIONALITY AND GLOBAL STANDARDS

AUTHORED BY - MAITRA VARUN CHOTIA,
PhD Research Scholar, Central Sanskrit University, New Delhi

Abstract

The paper presents a doctrinal study of the right to privacy in India, that is, its development over time by constitutional jurisprudence and statutory law. The paper looks at historic Supreme Court decisions such as *M.P. Sharma v. Satish Chandra* (1954), *Kharak Singh v. State of U.P.* (1963), [1]*Gobind v. State of M.P.* (1975), and most significantly *K.S. Puttaswamy v. Union of India* (2017) that resulted in the acknowledgment of privacy as the basic right in Article 21 of the Constitution[2]. It additionally discusses post-Puttaswamy privacy extensions to such matters as sexual (*Navtej Singh Johar v. Union of India*, 2018) and marital autonomy (*Joseph Shine v. Union of India*, 2019). At the statutory level, the paper examines such digital privacy laws as the Information Technology Act, 2000, the Aadhaar Act, 2016 and the recently introduced Digital Personal Data Protection Act, 2023. The DPDP Act is juxtaposed to the GDPR of the EU to evaluate its sufficiency with several issues being mentioned, including extensive governmental exemptions and the lack of sensitive data categories[3]. In comparative jurisprudence (and, it should be noted, a well-known case of it is Katz v. United States (1967)and Article 8 of the ECHR) is used in order to place position of India approach to the global privacy standards. [4]Findings of the research have shown that the Supreme Court has entrenched the concept of privacy in the domain of life and personal liberty; however, the Indian law fails to provide a strong rights-based regime on the protection of data. The paper ends with the recommendations on the refinement of the legislation laws, including the tightening of the enforcement system, reduction of the exemptions, and the closer correspondence to the international standards, which will help to make the right to privacy

[1] *Kharak Singh v. State of U.P. & Others*, AIR 1963 SC 1295 (Dec. 18, 1962), https://indiankanoon.org/doc/619152/.
[2] SCO Team, *Right to Privacy: Court in Review*, Supreme Court Observer (July 4, 2017), https://www.scobserver.in/journal/right-to-privacy-court-in-review/.
[3] Prabhash Dalei, *The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards* (2025), https://www.lawjournals.org/assets/archives/2025/vol11issue3/11064.pdf.
[4] Latham & Watkins, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison* (Dec. 2023), https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.

work more efficiently.

Keywords

Right to Privacy; Article 21; Data Protection; Puttaswamy; Aadhaar; Digital Personal Data Protection Act.

Introduction

The human right of privacy has become the cardinal human right of the digital era as it forms the foundation of human dignity, autonomy and integrity of personal life. Privacy has been acknowledged by international means: Article 8 of the European Convention on Human Rights provides the right to respect to private and family life, to his home and to his correspondence[5]. However, framers of the Constitution in India did not explicitly include a right to privacy. Another significant view of the early jurisprudence was that privacy was not an independent fundamental right under Part III. However, with the increase in technology and state authority, the Indian courts have come to the realization that privacy is implicit in the promise of life and personal liberty in the constitution (Article 21).

The paper presents a doctrinal survey of such an evolution. It looks at some of the landmark Supreme Court cases beginning with M.P. Sharma v. Satish Chandra. Through Kharak Singh v. State of U.P, in which an eight-judge Bench refused to read a Fourth Amendment-style right to privacy into the Constitution, the Court has not taken such a step. Even though it did not recognize an express right to privacy, quashed invasive police rules as infringing Articles 21[6]. The story goes on to Gobind v. The Court once more affirmed the right to surveillance laws in State of Madhya Pradesh (1975) but urged that they were taking a dangerous step towards unconstitutionality [7]. Modern age started with a case of K.S. Puttaswamy v. Union of India (Puttaswamy I) (2017), [8]the nine-judge Constitution Bench found in unanimity that privacy was an intrinsic component of Articles 14, 19 and 21[9].

[5] Council of Europe, *Right to respect for private and family life*, European Convention on Human Rights, https://www.coe.int/en/web/human-rights-convention/private-life.
[6] *Kharak Singh v. State of U.P. & Others*, supra note 2.
[7] *Gobind v. State of M.P. & Anr.*, AIR 1975 SC 1378 (Mar. 18, 1975), https://indiankanoon.org/doc/845196/.
[8] Columbia Center for Global Freedom of Expression, *Puttaswamy v. Union of India (II)*, Global Freedom of Expression Project, https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-union-of-india-ii/.
[9] SCO Team, *supra* note 2.

At the same time, the statutory regime in India has been following suit: the Information Technology Act 2000 includes, among other things, clauses criminalizing some privacy invasions (as in the case of voyeurism in Section 66E) and data-security provisions (in Section 43A). Intense debate over biometric identity was triggered by the Aadhaar Act 2016, which required it, and was partially affirmed in Puttaswamy (Aadhaar II) (2019). The latest Act is the Digital Personal Data Protection Act, 2023 (DPDP Act) which was made in order to regulate personal data on a large scale in the global trends such as the GDPR in the EU. The paper will examine these laws against the constitutional standards, whether they provide sufficient privacy safeguards. The analysis is informed by comparative jurisprudence. Although the strategy of India is based on Article 21, the parallels of the U.S. privacy law (e.g. Katz v. United States) can be drawn. The Fourth Amendment of the United States, which has infamously stated that the Fourth Amendment protects individuals, not property[10]) and European data protection regulations (GDPR; Article 8 ECHR) furnishes doctrinal background. The aim is to put the privacy doctrine of India into an international context, with the aim of demonstrating how the comparative principles can justify Indian constitutional values and not substitute them. This study, therefore, aims at mapping constitutional and legislative boundaries of privacy in India, to determine whether the law is in tandem with the doctrine of fundamental rights, and to propose changes to enhance privacy protection. The methodology, in the search of these aims, is doctrinal: it makes use of primary sources (Constitution, statutes, case law) and academic commentary. The paper summarizes the legal arguments based on judicial decisions and finds trends and gaps, the purpose of which is to create a thorough and authoritative treatment that could be published in a human rights law journal. The academic literature about the privacy law in India emphasizes the fact that the law is new and requires a solid structure. According to many commentators, until Puttaswamy (2017), privacy was frequently lost in other rights or statutory schemes.

As an example, Luthra and Bakhru note that Indian courts have been cautiously accepting the concept of privacy as a constitutional value and tend to consider rights such as publicity or intellectual property, in privacy-like terms[11]. A recent criticism of the new data protection law in India, the DPDP Act, is given by Dalei (2025), who points out the importance of the

[10] *Katz v. United States*, 389 U.S. 347 (1967), https://supreme.justia.com/cases/federal/us/389/347/.
[11] Samarth Krishnan Luthra & Vasundhara Bakhru, *Publicity Rights and the Right to Privacy in India*, National Law School of India Review, Vol. 31, Issue 1 (2019), https://repository.nls.ac.in/nlsir/vol31/iss1/6/.

Puttaswamy judgment in emphasizing the necessity to have a specific legal framework that would regulate data privacy [12].

He cautions, though, that the DPDP Act has significant loopholes: it does not include a special category of sensitive personal data, it has blanket exemptions to the State, and it sets up a Data Protection Board that is not independent enough. Such works indicate a literature that concerns the legislative reaction to Puttaswamy, but acknowledges that additional research is required on the constitutional doctrine. Indian law journals have also written critical articles that have followed the constitutional path of privacy. Before Puttaswamy, some writers had argued over whether privacy was amenable to being read into Article 21 or it could be trusted to as an unenumerated personal liberty. Indicatively, certain evaluations of Kharak Singh and Govind have found that as much as the initial instances overturned a free-standing right, they tacitly recognized privacy as the key to liberty. Some have also discussed particular aspects: Rajagopal (1994) was known to affirm privacy (in press context) under Article 21[13]. Since Puttaswamy, the scope of the new jurisprudence is the subject of articles. An example is that law review articles are expected to talk about Navtej Singh Johar (2018) as a continuation of privacy to sexual autonomy, [14]and Joseph Shine (2019) as a statement of personal dignity in intimate matters[15]. Academic discourse about the protection of data in the area of data protection focuses on the sufficiency of laws. Researchers compare Indian legislation that governs the privacy of the digital world to the international standards. When compared with the GDPR of the EU, it can be seen that the laws of India apply similar principles (consent, data minimization, user rights) but also have several significant differences - such as publicly available data is not subject to the law of India, and the processing is not based on the legitimate interests principle[16]. Certain commentary (e.g. privacyinternational, Hogan Lovells) points out that the scheme in India is still in its infancy and that key rules and mechanisms to enforce the scheme have yet to be developed. What comes out is there is a consensus that India is shifting towards an all-encompassing privacy regime, yet one where the legislative policy and the bureaucracy is still evolving.

[12] Prabhash Dalei, *supra* note 3.
[13] Columbia Center for Global Freedom of Expression, *R. Rajagopal v. State of Tamil Nadu*, Global Freedom of Expression Project, https://globalfreedomofexpression.columbia.edu/cases/r-rajagopal-v-state-of-t-n/.
[14] Columbia Center for Global Freedom of Expression, *Navtej Singh Johar v. Union of India*, Global Freedom of Expression Project, https://globalfreedomofexpression.columbia.edu/cases/navtej-singh-johar-v-union-india/.
[15] *Joseph Shine v. Union of India*, (Sept. 27, 2018) (reported as (2019) 3 S.C.C. 39), https://indiankanoon.org/doc/42184625/.
[16] Latham & Watkins, *supra* note 4.

It is required to bridge the gap between the role constitutional doctrine plays, and will play, in legislative privacy protections, and vice versa. Second, comparative views are usually made on a shallow level; an in-depth comparative analysis of the doctrines (i.e. how reasonableness under Article 21 parallels reasonableness under Article 8 jurisprudence) is seldom done. Lastly, the importance of the emerging case law under Puttaswamy and new law is evolving, and thus requires new analysis.

Research Methodology

The approach taken is the doctrinal legal research. It entails the methodical analysis of primary materials (the Constitution of India, statutes, and judicial decisions) and secondary materials (articles in law journals, commentaries, legal blogs, and international materials). It mainly deals with Indian Supreme Court jurisprudence and text of the applicable laws. Authoritative decisions are examined in terms of legal principles and reasoning whereas statutes are interpreted based on their contents and legislative intent. Where relevant, other jurisdictions that share similar legal principles are consulted to provide an example of similar principles (such as cases of the Fourth Amendment of the United States, rules on data protection in the European Union, and rights rules in the Council of Europe).

Legal database search and open-source legal analysis was used to collect data. Cases of great judicial importance (Puttaswamy, Johar, etc.) were read in full; key passages were pointed out and quoted verbatim. The recent laws (Aadhaar Act, DPDP Act) were found on government websites and academic summaries. Academic databases and repositories (e.g. NLSIR, journal websites) were used to identify law review and journal articles. Comparative jurisprudence was based on the standard texts (e.g. Katz, GDPR text) and official commentaries. The analysis will be done in thematic manner to follow the doctrinal evolution of privacy and to cover all aspects of the constitutional, legislative and comparative matters.

I. Preliminary Constitutional Jurisprudence

The privacy was not guaranteed in the original Constitution. The 1954 ruling in M.P. Sharma v. Satish Chandra (The eight-judge bench) determined that the framers of the Constitution did not mean to interpret an Indian law Fourth Amendment-type privacy right. The Court indicated that protection of personal liberty by Article 21 did not restrict searches and seizures by police, as those who drafted the Article did not intend to make the power of search and seizure a fundamental right of privacy. that is, M.P. Sharma stated that privacy was not a fundamental

right guaranteed in 1954 and analogies to the Fourth Amendment of the US Constitution were not intentionally made.

Less than ten years later, this issue was reconsidered in Kharak Singh v State of U.P, the Court in Kharak Singh had to deal with the police rules that allowed nocturnal surveillance and entry. Most of them reiterated the stand of M.P Sharma: right of privacy is not a right which is guaranteed in our Constitution. Nevertheless, most of them also acknowledged that the personal liberty under Article 21 is wide. The judges believed that personal liberty refers to the absence of restrictions or encroachment on his person and unchecked police surveillance may be an infringement of Article 21. As a result, the unconstitutionality of the Regulation 236(b) that confirmed midnight home visits (no law authorizing it) and the other surveillance provisions survived. Notably, the Kharak Singh majority construed Article 21 to implicitly safeguard the domestic and physical integrity of the citizens although it did not provide privacy as a stand-alone right. The concurrence view by Justice Subba Rao, even extended further, to state that privacy is a necessary component of the liberty of the person, but he was not a majority. Therefore, Kharak Singh set out that privacy as such was not guaranteed but that under Article 21, extreme intrusion by the State could be checked.

In Gobind v. State of M.P. (1975), the Court dealt with such regulations by the police. The Court dismissed the petition to invalidate the rules, but nonetheless, strongly cautioned that some of the regulations were looking dangerously close to being unconstitutional. It confirmed that Article 21 stipulates that a legitimate law has to be in place that permits surveillance, and that excessive and unmonitored surveillance is an infringement on individual freedom. The Court also limited police authority by interpreting the regulations as they were narrowed to particular extent (e.g. limiting domiciliary visits to unclear security cases). Therefore, Gobind provided an example of a practical solution: despite the lack of mentions of privacy, the laws had to be interpreted strictly to consider the individual freedom.

The other milestone was that of R. Rajagopal v. State of Tamil Nadu (AIR 1995 SC 264) which concerned the freedom of press and the defamation of a public personality. The Court acknowledged the value of privacy as a constitutional right as opposed to property rights. It claimed that the right to privacy of an individual was guaranteed under the Constitution as a fundamental right but not absolute. This was restricted to the press situation, but it indicated the Supreme Court was ready to recognize an implied privacy right in Article 21 (usually citing

the Latin maxim of protecting personal property against illegal government invasion). The Rajagopal Court citing Kharak Singh observed that protection of privacy is provided by both the tort law and the constitution. Therefore, as early as the mid-1990s, Indian jurisprudence already started to accept privacy in certain situations, which predicted the wider change in Puttaswamy.

The pattern of these cases is: hesitation in M.P. Sharma was replaced by a more liberal interpretation of Article 21 in Kharak Singh and Rajagopal, between the dignity and liberty of the individual and the power of the state. Initially, courts perceived privacy in a limited manner, but over time gave an opportunity to privacy-related claims in the frames of the existing rights (life, liberty, expression). This theoretical background prepared a clear-cut solution in Puttaswamy.

II. Article 21 and K.S. Puttaswamy Judgment (2017)

Justice K.S. Puttaswamy (Retd.) was the watershed in the Indian privacy law. In the case of Puttaswamy I, a question on whether privacy was essential or not was referred to a larger nine-judge Bench by an eight-judge bench. The Court decided on August 24, 2017 that privacy is a basic right, and is inherent in Articles 14, 19 and 21 of the Constitution. The Puttaswamy I Court clearly reversed previous dicta to the contrary (M.P. Sharma, Kharak Singh), reinstating the dissenting opinions that privacy was implicit in human dignity and freedom. [17]The dignity, as one of the opinions agreed, cannot exist without privacy and privacy is the ultimate embodiment of the sanctity of the person[18].

Altogether, Puttaswamy I has defined the privacy as an inherent aspect of the right to life and personal liberty in the Article 21[19] with a strong back up. The rationale behind the judgment resonated with the international standards: by citing U.S. precedent, it stated that the person has reasonable expectation of privacy even in a public place (we do not sit in judgment of him the injured person simply because we think he deserves privacy in the telephone booth). The universal implication can be seen in the fact that Justice Chandrachud notes that the Fourth Amendment does not guard places, but individuals - an American saying that highlights the subjective right to privacy. On the same note, the Court referred to Article 8 of the European

[17] *Joseph Shine v. Union of India*, *supra* note 15.
[18] Id.
[19] Columbia Center for Global Freedom of Expression, *supra* note 8.

Convention, which states that the ECHR courts safeguard a wide privacy area. Puttaswamy judgment, therefore, interprets Indian doctrine in these comparative principles, and it grounds such principles on the Constitutional text of India.

Since Puttaswamy all the new dimensions of personal choice have been put to the test of privacy. Notably, In Navtej Singh Johar , laws that criminalize consensual homosexual behavior were declared illegal by the Supreme court. The Court believed that sexual orientation is part and parcel of privacy and personal identity; the prohibition of privacy, consensual sex between adults was against both dignity and privacy in Article 21. Likewise, In Joseph Shine v. Union of India (2019), the adultery law (IPC SS497) was invalidated by Union of India (2019), which focused on personal autonomy and marital privacy.[20] The Court in Shine recognized that adultery was at the lowest point of individual self-determination and that the government had no right to interfere with marital privacy[21]. These examples demonstrate how the privacy principle developed by Puttaswamy has proven to be a reference point in numerous situations, safeguarding personal decisions and physical privacy against the moralistic or protective law.

III. Data Protection and Statutory Framework

In addition to the Constitution, Indian laws have over time dealt with privacy particularly in the digital world. There are a number of provisions on privacy in the Information Technology Act, 2000 (with an amendment in 2008). Section 43A requires that some corporate organizations that hold sensitive personal data or information should put in place reasonable precautions to safeguard the same or pay damages in case of failure - a precursor acknowledgment of an informational privacy interest. Section 72A punishes such breach of lawful contract by a service provider disclosing personal data. Section 66E, which was enacted in 2008, makes it a criminal offense to capture and publish the image (including nudity) of a private person without their consent. These clauses are an indication that the legislature has acknowledged the presence of privacy breaches (particularly digital) as an element deserving legal penalties, but in a compensatory or punishment context, as opposed to a rights-based approach.

[20] *Joseph Shine v. Union of India*, *supra* note 15.
[21] *Joseph Shine v. Union of India*, *supra* note 15.

Markedly, though, there are other provisions of the IT Act that permits extensive state surveillance. In sections 69 and 69A, the government is given the powers to intercept, monitor or decrypt any information in the interest of sovereignty or security, provided it is done under procedural requirements (e.g. approval by a competent authority). According to critics, these provisions are mostly beyond judicial scrutiny and may be abused. Therefore, the privacy (through data security provisions) and also the enabling intrusion (through surveillance provisions) are both safeguarded by the IT Act. This duality is indicative of a precarious compromise between personal privacy and national security in the former laws.

India has a biometric ID system, which was created through the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Since biometric and demographic data are gathered in large numbers, Aadhaar served as the point of privacy anxieties. This was considered by the Supreme Court in the case of Puttaswamy (Aadhaar II) (2019). Most of them affirmed major requirements - such as the need to use Aadhaar to access select welfare schemes (Section 7) and the acknowledgment of Aadhaar numbers as sensitive personal data under the Act - but invalidated others. [22]The Court invalidated the requirement to link Aadhaar and PAN numbers with SIM cards and bank accounts by e-KYC because such requirements were beyond the intention of the law[23]. It also restricted data storage (e.g. not more than six months of some UIDAI data). The judgment of Justice Sikri was famous as he supported the use of Aadhaar in entitlement but concluded that the Act does not establish a system of omnipresent surveillance by the State. Justice Bhushan concurred with Section 7 and passed the Puttaswamy test in concurrence: he saw a legitimate state interest in the competent welfare provision and considered compulsory Aadhaar reasonable to subsidies, but he did not agree on certain provisions. Therefore, the Aadhaar decision upheld the legality of the identification effort by the government, but established that it was necessary to ensure that the effort was not made without the principles of privacy (such as necessity and minimal intrusion). It was made clear in the case that even social welfare laws should be subjected to Article 21 in the case of personal data.

The Data Protection act, 2023 (DPDP Act) is the first data protection law in India. It was

[22] SCO Team, *Constitutionality of Aadhaar Act: Judgment Summary*, Supreme Court Observer (Sept. 26, 2018), https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/.
[23] Id.

enacted in August 2023, following Puttaswamy and international demands on data regulation. The DPDP Act is a broad definition of digital personal data and provides a responsibility on data fiduciaries (entities that exercise control over data) and data principals (individuals). It gives rights of access, correction and grievance redressal to the data principals and fines against violations. The Act contains express concepts of consent, a limited purpose, and minimum data reduction - concepts that are quite comparable to the EU GDPR[24]. As an example, a fiduciary is required to get the free, informed, specific, clear and capable of withdrawal consent of the data principal (similar to the GDPR standard).

Nontheless, the DPDP Act has significant differences when compared to the GDPR. India, as Dalei notes, does not include publicly available personal information in its law, and the GDPR includes publicly shared information (with certain exceptions). Additionally, as opposed to six legitimate bases of processing permissible under GDPR (consent, contractual necessity, legal obligation, vital interests, public task, legitimate interests), the DPDP Act permits processing solely by consent or based on a restricted set of legitimate purposes (e.g. business operations, employment, public interest). This more limited ground, though strengthening consent, deprives the more liberal test of the GDPR of legitimate interests, which may limit business applications. New rights specific to India are also introduced by the Act: all data fiduciaries should have a Grievance Redressal Officer to deal with complaints, such as, nod to India, a nod to consumer grievances tradition.

Such critiques as Dalei (2025) observe that the DPDP Act, however progressive in terms of codification of privacy norms, has some serious exemptions. As an illustration, it permits the government to manipulate individual data towards some state purposes, which seemingly do not need to be well-supported. It also lacks a special category of sensitive personal data, as the original 2019 Bill or GDPR does. Moreover, the regulatory body (the Data Protection Board) of the Act lacks powers to investigate until the rules are framed. Such gaps have prompted commentators to warn that in practice the law will not be as protective as it is supposed to be. As an illustration, an expert comparison observes that India DPDP Act does not specify the data portability or a required reporting period, as GDPR[25] does. Overall, as much as the DPDP Act reflects a constitutional acknowledgment that data privacy needs to be regulated (a reaction

[24] Latham & Watkins, *supra* note 4.
[25] Prabhash Dalei, *supra* note 3.

to the Puttaswamy and world trends), the current version can be considered an outline of the privacy legislation and not a complete one.

IV. Comparisons in Data Protection internationally

The GDPR (Regulation (EU) 2016/679) is a relatively high standard of data rights and has affected the approach of India. The two laws will guarantee the rights of data principals and hold fiduciaries (controllers) accountable. However, as it has been mentioned, the GDPR extends its reach past the territorial boundaries of the country and includes such notions as the adequacy decisions to cross-border transfer, which the Indian scheme does not have today. Article 8 ECHR does not refer to it directly on Article 8 ECHR, but the spirit of Article 8 ECHR is echoed in Indian case law. As an example, the European courts have considered that the simple gathering of personal information by the state authorities should meet the proportionality condition; Puttaswamy also took a proportionality test to privacy violations (with references to Article 8 jurisprudence). The common law system of the U.K. (e.g. Campbell v. , MGN, 2004] EWCA Civ 37 Similarly to the developing right to privacy in India) considers privacy as a tort under the human rights law.

V. Privacy vis a vis the Indian constitution

Privacy is overlapped with other provisions of the constitution. The example of article 19(1)(a) (expression) suggests a limited right to free speech in private (e.g. PUCL v.UOI) and the Supreme Court has upheld anonymity in speech (e.g. PUCL v.. Union of India, 1984). The jurisdiction of the article 21 itself is broad: privacy has been associated with dignity and autonomy of life. In Puttaswamy and Johar the Court referred to the dignity in the Preamble to support privacy. More so, Article 21 intersects with Article 14 (equality) in cases when the laws on privacy seem to be discriminatory; in Shine, the adultery law being gender-based breached the equality and consequently the dignity and privacy of women.

Overall, the constitutional doctrine of privacy of India has now been firmly rooted in Article 21 (under the support of Articles 14 and 19), which has led to a range of privacy-protected interests: between bodily integrity and information privacy. The laws such as the IT Act and the Aadhaar law have gradually acknowledged the issue of privacy, albeit in specialized plans. The new DPDP Act is a holistic statutory initiative though still lagging behind constitutional promises. The comparative law demonstrates that Indian trends are congruent with the global

human rights (with India adopting Katz-like reasonable expectation and proportionality) and that Indian statutory gaps are no different than in other countries: early GDPR-like legislation (as it was enacted) frequently left the enforcement details to further regulations.

VI. Findings and Suggestions

In this study, it is established that the right to privacy in India has grown to become a constitutional right, through a consistent jurisprudence of Article 21. Privacy is now considered a fundamental right by the Supreme Court, which encompasses personal autonomy (decisional privacy) as well as informational privacy. All the personal freedoms, such as personal relations (Johar) and body integrity (Shine) are safeguarded. Notably, privacy is not a minor right anymore, as it is subordinated by others, but rather has its own status and established boundaries (legality/necessity/proportionality). Statutorily, India has passed a specific law on data protection (DPDP Act 2023), other pieces of legislation have been passed that deal with some privacy concerns. Nevertheless, the legislative framework is still a developing one. The existing laws are not as mature and comprehensive as the major international standards (such as the GDPR has more developed accountability measures and extended individual rights). The trade-off between privacy and other values (such as security or welfare) should be constantly adjusted policy-wise. The jurisprudence reveals that the Court is ready to invalidate state actions that unjustifiably violate privacy and acknowledge the valid state purposes. The review of Aadhaar revealed the following balance: on principle, government welfare needs were a sufficient condition to have a central biometric database, but non-welfare applications of Aadhaar did not pass privacy tests. In the future, legislatures need to embrace the Court tripartite test when writing laws that are related to personal data or surveillance. This may involve incorporation of the so-called Puttaswamy compliance clauses in new legislation, or changing current legislation (e.g. IT Act, Telegraph Act) to stipulate that data collection and surveillance require authorization by law, legitimate purpose, and proportionality. Recommendations on data protection include: reducing statutory exemptions to avoid blanket privacy waivers; treating sensitive personal data (health, biometrics, etc.) as a separate category to give it greater protection; and making the Data Protection Board more independent as an analog of a regulator (like Data Protection Authorities under GDPR). The penalties and remedy pathways also require definition in India: at the moment, the DPDP Act is considering the fines but the redress mechanism is not well-developed. Enforcement - by allowing class actions or strengthening civil courts, etc. - would be more effective in deterring.

On a larger scale, there is the role played by awareness of the people and digital literacy. The right to privacy cannot be valid when citizens are unaware of them. Legal reforms, therefore, are to be accompanied by education and a culture of data responsibility by businesses and government. Risks in the digital economy can be also diffused by encouraging privacy-enhancing technologies (encryption, data anonymization).

To sum up, the right to privacy in India is constitutionally safe and acquires new jurisprudential significance. But to make full effect of this right in practice, there must be gaps to be filled in by the law. It requires a more dynamic approach: the boundaries of privacy still must be drawn on a case-by-case basis by the courts, and the law on privacy must be improved by legislatures, with expert and civil society advice. Privacy protection will be reinforced by including comparative best practices (based on GDPR, ECHR, etc.), where they are compatible with the Indian values. This concerted effort will see to it that in India, the security of privacy, is actually considered to be basic to a free society - as it is envisioned in both domestic and international jurisprudence[26] .

Bibliography

- *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
- *Kharak Singh v. State of Uttar Pradesh*, AIR 1964 SC 1295.
- *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
- *R. Rajagopal v. State of Tamil Nadu*, AIR 1995 SC 264.
- *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 SCC 1.
- *K.S. Puttaswamy (Retd.) & Anr. v. Union of India (Aadhaar)*, (2019) 1 SCC 1.
- *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.
- *Joseph Shine v. Union of India*, (2019) 3 SCC 39.
- Constitution of India art. 21; Information Technology Act, 2000 (No. 21 of 2000); Aadhaar Act, 2016 (No. 18 of 2016); Digital Personal Data Protection Act, 2023 (No. 10 of 2023).
- Samarth K. Luthra & Vasundhara Bakhru, *Publicity Rights and the Right to Privacy in India*, 31 NLSIR 137 (2019).
- Prabhash Dalei, *The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards*, 11 Int'l J. Law 127 (2025).
- Global Freedom of Expression, Columbia Univ., *Puttaswamy v. Union of India (II)* (Sept.

[26] Columbia Center for Global Freedom of Expression, *supra* note 8.

2018) (case commentary).

- Global Freedom of Expression, Columbia Univ., *Navtej Singh Johar v. Union of India* (Sept. 2018) (case commentary).

- Council of Europe, *European Convention on Human Rights*, art. 8 (1950).

- Katz v. United States, 389 U.S. 347 (1967).

- GDPR: Regulation (EU) 2016/679 of 27 April 2016.