INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

ISSN: 2582-6433

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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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.

ISSN: 2582-6433

RIGHT TO PRIVACY IN INDIA: EVOLUTION FROM KHARAK SINGH TO PUTTASWAMY

AUTHORED BY - AYESHA SIDDIQUI
DESIGNATION- Student
UNIVERSITY - Amity University, Lucknow

Abstract:

The evolution of the right to privacy as a fundamental right in India has been incremental but revolutionary in nature, influenced by judicial perception as well as changing needs in society. The Supreme Court initially declined recognizing the existence of privacy as a constitutionally protected right in **M.P. Sharma v. Satish Chandra**[1] and **Kharak Singh v. State of Uttar Pradesh**[2], in which the focus still persisted on state authority as well as due process instead of the liberty of individuals. But the tide in jurisprudence slowly started changing in **Gobind v. State of Madhya Pradesh**[3], in which the Court carefully demonstrated privacy under the parameters of personal liberty under Article 21, though open to reasonable limitations.

This incremental evolution opened the way to later deliberations in the judiciary, leading to the historic **Justice K.S. Puttaswamy v. Union of India**[4] judgement, when nine judges unanimously declared the right to privacy as a constitutionally embedded fundamental right integral to dignity, liberty, as well as autonomy.

This research paper critically explores this evolution in the jurisprudence of privacy in India, tracing the thread of constitutional philosophy in the rulings, the interaction between state power and individual rights, as well as the increasing impact of comparative as well as international jurisprudence. Through these analyses, the research underlines the abiding tension between protecting individual liberty as against accommodating legitimate state interest in spheres like national security, public order, as well as good governance.

[1] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300
[2] Kharak Singh v. State of Uttar Pradesh, 1963 AIR 1295
[3] Gobind v. State of Madhya Pradesh, 1975 AIR 1378
[4] Justice K.S. Puttaswamy v. Union of India, AIR 2018 (SUPP) 1841

ISSN: 2582-6433

The paper concludes that privacy is not just a derivative right but a vital part of human dignity, autonomy, and democratic engagement in the constitution. Recognition of this right is significant in the constitutional democracy in India as that showcases the judiciary's efforts to evolve the fundamental rights to meet the needs of the current digital age.

Keywords: Right to Privacy, Fundamental Rights, Article 21, Data Protection, Surveillance, Indian Constitution, Human Dignity.

1. Introduction:

The Indian Constitution, while embracing a wide collection of basic rights, technically fails to mention the **"right to privacy."** But as the jurisprudence under the Constitution has evolved, courts have gone decisively to read privacy in the substance of the right to life and liberty under **Article 21**. This evolution from blanket rejection to vigorous affirmation witnesses one of the most fascinating transformations in the law under the Constitution for India.

The right to privacy is not only a product of law but a profoundly philosophical and moral concept based on human dignity, liberty, and autonomy. Privacy has taken unprecedented significance in the era of globalization, rapid technological advances, and large-scale surveillance. Questions relating to protection of data, governmental surveillance, and individual freedoms have redrafted the parameters of constitutional law and posed important questions about the fine line between individual rights and national security.

The jurisprudence of privacy in India can be traced as the narrative of three stages:
(i) **rejection** of privacy as a fundamental right in the early cases; (ii) gradual, conditional **recognition** in the 1970s and in the 1990s; and (iii) recognition of privacy as a **fundamental right** in Justice K.S. Puttaswamy v. Union of India. All these stages are indicative of changing attitudes in the courts towards liberty as well as towards constitutionalism.

This paper maps this evolution from Kharak Singh through to Puttaswamy, tracing the constitutional foundations, judicial reasoning, and broader implications for government and democracy in India. It also intersects with comparative methodologies, international human rights norms, and contemporary challenges in attempting to predict the future course of privacy in India.

ISSN: 2582-6433

2. Right to Privacy- It's nature

The nature of the right to privacy has long been in controversy, with doubt as to whether it is an ordinary statute-based right or possesses the superior status of a fundamental or constitutional right. Courts have again and again struggled to define its extent and to determine when a violation might be formally acknowledged as the law. Without clear mention in the constitution, recourse to foreign courts was often sought by judges in search of guidance, only to discover that few nations specifically secure privacy.

Privacy has thus developed overwhelmingly through the courts, gradually taking shape on an ad hoc case-by-case basis, i.e. a matter is not handled according to a fixed rule, system, or general policy, but instead is decided individually for each situation as it arises, often in a temporary or improvised way. This renders judicial thought the unifying driving power in its evolution, as courts, in response to change in society and advances in technology, have progressively provided the concept with increased distinctness as well as significance.

The history of privacy has mirrored the recognition of other derivative rights like the right to food, to health, to environment; which were not themselves listed in the constitution but were inferred from broader provisions for liberty and dignity by the courts. As a result, privacy has shifted from being an **ambiguous and unclear**, disputed right to something more **settled, clear and enforceable.**

3. Early Judicial Approach:

The Indian judiciary first applied the doctrine of privacy in M.P. Sharma v. Satish Chandra, where the Supreme Court reflected upon the constitutionality of search and seizure under **Article 20(3)**[5]. The issue was if the petitioner had a right to privacy in light of a search being conducted at his premises without notice, thereby violating his private space.

The court here referred to the aspect of 4th Amendment of the United States Constitution for guidance. An eight-judge bench categorically held that the Constitution of India does not grant the right to privacy as a fundamental right.

The Court observed that whereas the U.S. Constitution has specifically engraves protection

[5] fundamental right against self-incrimination

ISSN: 2582-6433

from unreasonable searches and seizures in the Fourth Amendment, nothing like that was to be found in the Indian Constitution. Privacy as a fundamental right therefore could not be read from the text. The decision was important in reflecting the court's reluctance to interpret the rights under the constitution any deeper than the text's manifest provisions. The strict text approach was in sharp contrast from later liberal interpretations on Article 21.

The real foundation of privacy jurisprudence in India was laid in Kharak Singh v. State of U.P., wherein the petitioner who was under suspicion in criminal cases challenged the police regulations that allowed domiciliary night visits and surveillance. In this case the issue of privacy came up in the context of a prisoner who had been charged with the offence of dacoity and later acquitted due to insufficiency of evidence.

His movements were watched even after being acquitted and surprise visits were conducted to his house at irregular intervals, this being provided under **Regulation 236 of UP Police regulations.** The majority decision i.e. the seven-judge bench, that of Justice Ayyangar, was that this right to privacy was not a fundamental right as per the constitution. But the Court held domiciliary visits to be unconstitutional since these violated the "personal liberty" which is afforded to citizens under Article 21.

It is significant that the **minority report** by Justice Subba Rao recognised the right to privacy in the right to liberty. He suggested that:
"The right to personal liberty takes in not only the right to be free from restrictions placed on his movements, but also free from encroachments on his private life." This difference of opinion was to provide the germ for the later recognition of privacy. Thus, Kharak Singh marked a paradox: while the majority denied privacy as a constitutional right, the minority's reasoning laid the foundation for its eventual recognition.

The court refused to interpret Article 21 as including right to privacy due to the binding opinion rendered in **A.K. Gopalan v State of Madras**[6], where it was held that fundamental rights **do not have the attribute of travelling entities** i.e. each fundamental right guaranteed under a specific provision is confined to it and nothing more can be imputed/inferred.

[6] A.K. Gopalan v State of Madras, 1950 AIR 27

ISSN: 2582-6433

Hence, the court here contradicted itself while admitting the surveillance of the movements of an individual to be a violation of Article 21 and at the same time denying a right to privacy.

4. Gradual Recognition of the Right to Privacy:

In the beginning, refusal to act on the Constitution was what we termed as the **'Jurisprudential Phases of the Right to Privacy'** in India. However, there was a significant change in the 1970s. This was the time when the Indian judiciary, particularly after the case of **Kesavananda Bharati v. State of Kerala**[7], began interpreting the fundamental rights with a more liberal and expanded approach. Considering the sustained apprehension of the safeguarding of individual rights and freedom against the extending peeping of the State, the courts started accepting privacy as a constitutional value.

The Supreme Court in Gobind v. State of M.P. was called upon to answer the question whether the police surveillance sanctioned under the Madhya Pradesh Police Regulations is constitutionally permissible. Constant police surveillance was challenged by the petitioner as derogatory to his fundamental rights under Articles **19(1)(a)**[8]**, 19(1)(d)**[9]**, and 21**. Justice Mathew, in writing for the Court, noted that while the Constitution did not specifically grant the right to privacy, the latter can still be inferred in the basic rights.

The Court held that the right to life and personal liberty under Article 21 implicitly embraced the right to privacy as did the freedoms under Article 19. But this inclusion was not unwavering. The Court held that the right to privacy can be shortened off in the higher state interest in the form of public order as well as security. The Court observed:
"If liberty of the person, liberty to move anywhere in the entire territory of India, liberty of speech constitutes an independent right to privacy; then this is in practical effect only the right 'to be let alone.' But the privacy shall be subordinated to superior public interest."

Hence, Gobind marked a turning point, it conditionally acknowledged the right to privacy, setting it against the needs of the community. It also took the case-to-case stance, leaving to later courts to clearly define the outlines of privacy.

[7] Kesavananda Bharati v. State of Kerala, AIR 1973 SC 1461
[8] Right to freedom of speech and expression
[9] Right to move freely throughout the territory of India

ISSN: 2582-6433

The Supreme Court in **Malak Singh v. State of Punjab**[10] dealt with police tracing of habitual offenders. While affirming tracing in principle, the Court cautioned that tracing ought to be carried on in such a manner that dignity as well as privacy of individuals are not infringed more than is absolutely necessary. The decision reaffirmed once again that **dignity is commensurate with privacy**, that though the State can dictate in the interest of safety, this right is not absolute. The case was typical of increased judicial reluctance to shield citizens from unworthy intrusions into their lives by police departments.

Perhaps one of the most significant cases in the evolution of privacy was **R. Rajagopal v. State of Tamil Nadu**[11]. Popularly known as the **"Auto Shankar" case**, it involved a convicted prisoner who wrote his autobiography detailing links between criminals and prison officials. The prison authorities sought to prevent its publication in a magazine.

The Supreme Court has held that the right to privacy is hidden in the right to life and liberty under Article 21. The court has also made clear that privacy entails the right to protect personal affairs, family life, as well as correspondence from unwarranted intrusion. But where the subject matter is part of the public domain, publication thereof cannot be enjoined. It held that: "The right to privacy is the right to be let alone. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education, among other matters."

This case firmly established privacy in the context of free speech and freedom of the press under Article 19(1)(a). It drew a balance between press freedom and the individual's right to private life, setting the stage for broader recognition in later judgments.

In **PUCL v. Union of India**[12], the Supreme Court discussed the telephone tapping and its constitutionality. The petitioners argued that indiscriminate tapping of telephones was against the right to privacy. The Court agreed, ruling that tapping of telephones violates the right to privacy under Article 21 unless done in accordance with a fair, just, and reasonable procedure. The Court asked the government to draft guidelines to govern tapping of telephones, stating that privacy cannot be restricted arbitrarily. This was a pioneering judgment in that it

[10] Malak Singh v. State of Punjab, 1981 AIR 760
[11] R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264
[12] PUCL v. Union of India, AIR 1997 SC 568

ISSN: 2582-6433

acknowledged informational privacy within communications, anticipating future issues in the digital era.

5. Intersecting spheres of fundamental rights:

One of the primary reasons for the rejection of the right to privacy as an independent right in the Kharak Singh case was the Court's reliance on the precedent set in A.K.Gopalan v. State of Madras. In Gopalan case, the judiciary had taken the view that fundamental rights were to be interpreted strictly within the confines of their specific provisions, thereby disallowing the recognition of new rights or the overlapping of existing ones. This rigid interpretation, however, was later overturned. In **R.C. Cooper v. Union of India**[13], an eleven-judge bench rejected the compartmentalized approach, and the principle was further reinforced by a seven-judge bench in **Maneka Gandhi v. Union of India**[14]. Both these landmark rulings emphasized that fundamental rights cannot be restricted to isolated silos; rather, their overlapping nature is both valid and constitutionally permissible.

6. The turning point in the evolution of the Right to Privacy:

The establishment of privacy as a constitutional right came to the point of decision in Justice K.S. Puttaswamy (Retd.) v. Union of India. The case was initiated by challenges to the Aadhaar scheme, a biometric identification system launched by the Indian government. Petitioners claimed that the storage and collection of biometric information like fingerprints and iris scans violated the right to privacy of citizens.

The Union of India, though, argued that as the Constitution did not clearly enshrine the right to privacy, no such constitutional right existed. This reignited the early decisions of M.P. Sharma and Kharak Singh, which had rejected privacy as a constitutional right. The seriousness of the constitutional issue resulted in the referral of the issue to a nine-judge bench of the Supreme Court.

The central issues before the court were:

i. Whether the Constitution of India guarantees a fundamental right to privacy;
ii. If so, what is the scope and content of this right? and

[13] R.C. Cooper v. Union of India, 1970 AIR 564
[14] Maneka Gandhi v. Union of India, 1978 AIR 597

ISSN: 2582-6433

iii. How should this right be balanced against competing state interests such as security, welfare, and transparency?

In a 9-0 unanimous judgment, the Supreme Court categorically held that the right to privacy is a fundamental right, inherent in the right to life and personal liberty under Article 21, and a part of the freedoms enshrined in **Part III of the Constitution**.

The Court specifically overruled M.P. Sharma and the majority in Kharak Singh, holding that their refusal to give recognition to privacy was unfavourable to constitutional philosophy. Justice D.Y. Chandrachud, speaking for the plurality, stressed that **privacy is intrinsic to human dignity**. It involves the right to make choices on a personal level, ownership over personal information, and the inviolability of personal spaces. The judgment also listed three dimensions of privacy:

(i) Spatial privacy (shield against intrusion into one's physical space);

(ii) Decisional privacy (autonomy to make personal decisions, e.g., marriage, procreation, or sexual orientation).

(iii) Informational privacy (autonomy over disclosure and utilization of personal information.

The Court ruled that **privacy is not absolute**. Similar to other basic rights, it can be limited by law subject to the condition that such limitation meets tests of legality, necessity, and proportionality. Privacy was not separable from Article 14, 19, and 21 freedoms. For example, freedom of expression encompasses right over dissemination of one's own personal information, and equality entails an understanding of privacy irrespective of class.

7. Impact of the Justice K.S. Puttaswamy (Retd.) v. Union of India judgement:

- Confirmatory of Privacy as a Fundamental Right: Privacy was at long last declared to be a constitutional right, putting it on par with other fundamental freedoms.
- Strengthening of Article 21 Jurisprudence: The judgment furthered the scope of Article 21, affirming its status as a reservoir of rights as opposed to specifically listed rights.
- Influence on Later Cases: **Navtej Singh Johar v. Union of India**[15]: Decriminalized homosexuality with a focus on decisional privacy and sexual autonomy. **Joseph Shine**

[15] Navtej Singh Johar v. Union of India, AIR 2018 SC 4321

ISSN: 2582-6433

v. Union of India[16]: Overturned law of adultery, upholding decisional privacy in personal relationships. **Common Cause v. Union of India**[17]: Established the right to die with dignity and living wills, rooted in privacy and autonomy.

- Advocacy for Data Protection Legislation: The ruling recognized informational privacy as a fundamental issue in the modern digital era. It initiated legislative action, such as the Personal Data Protection Bill (2019) which was later withdrawn by the Indian government on August 3, 2022, to be replaced by a new, more comprehensive bill. India subsequently passed the Digital Personal Data Protection Act (DPDPA) in 2023, which came into effect in 2024, establishing a new data privacy law.

The Puttaswamy judgment represents a constitutional milestone. It not only restored faith in the transformative vision of the Constitution but also adapted constitutional rights to modern challenges of surveillance, data collection, and digital intrusion. By rooting privacy in dignity, autonomy, and liberty, the Court ensured its universal application across contexts.

Yet, challenges remain. The judgment left open questions about the limits of surveillance, the scope of data protection, and the standards of proportionality. Moreover, practical enforcement of privacy rights continues to face hurdles, especially with the rise of state-centric technologies like Aadhaar, facial recognition, and digital monitoring.

8. Effect of enforcement of Right to Privacy:

In order to comprehend the change in the privacy regime in India, specifically in the pre- and post-period of the declaration of the fundamental right to privacy in K.S. Puttaswamy v. Union of India, certain empirical indicators need to be considered. The table below provides a general idea of the changes in the variables of digital penetration through Aadhaar, data breach reports, legal protection, and awareness in the pre- and post-period of 2017. Although some of the data is based on general trends, it is essential in understanding the broader change in the regime of privacy in India.

[16] Joseph Shine v. Union of India, AIR 2018 4898
[17] Common Cause v. Union of India, AIR 2018 SC 1665=

ISSN: 2582-6433

Year	Phase	Aadhaar Users (Millions)	Reported Data Breaches	Legal Protection Index (1-10)	Public Awareness Index (1-10)
2015	Pre	900	50	1	2
2016	Pre	1100	70	1	2
2018	Post	1200	120	3	5
2020	Post	1250	200	5	6
2023	Post	1300	350	7	8

A cursory observation from the table shows that there has been a steep rise in the number of data breaches, from 50 cases in 2015 to 350 cases in 2023. On the surface, the steep rise might seem to imply a decline in the level of privacy. However, the above observation does not fully capture the real dynamics of the situation. The parallel growth of the number of Aadhaar enrolments, from 900 million to 1.3 billion, shows the immense growth of digital engagement. The more the number of people access digital mediums, the more the amount of personal data created, thereby increasing the chances of data breaches.

More importantly, the post-2017 period marks a notable improvement in the legal and institutional framework with respect to privacy. This can be deduced from the rising scores of the Legal Protection Index, which has moved from 1 during the pre-2017 period to 7 as of 2023. The constitutionalization of privacy has forced the State to prove the legality, necessity, and proportionality of any invasion of privacy. In parallel, the Public Awareness Index has also recorded a notable increase, suggesting that the public has started becoming more aware of their rights and are taking a more assertive approach towards the violation of the same.

Consequently, it is important to understand that the increase in data breaches is not indicative of the failure of the privacy regime but is, in fact, a reflection of the transition to increased transparency and accountability. In the pre-2017 world, the lack of clear identification of the right meant that there was under-reporting and no recourse. However, in the post-Puttaswamy world, there is an environment that is characterized by visibility and contestability of privacy violation. Therefore, the data is a reflection of the transition from invisibility to visibility and regulation, which is characteristic of the dynamic nature of the evolution of privacy.

ISSN: 2582-6433

9. The concept of Data Privacy:

Data privacy has occupied a central place in recent times due to the rapid advancement in information and communication technology and the whole world being available with one click of the mouse. While it has made life much easier in terms of making efficient and economical modes of exchange and transmission of information from one place to another, it also calls into question the aspect of **"informational or data privacy."**

Informational or data privacy has become much vital in the recent times due to a large amount of information being collected by the state as well as private entities. Be it social networking websites such as Facebook, banks, hospitals, restaurants etc, each one of them has substantial information collected on a particular individual. The establishment of the right to privacy in Justice K.S. Puttaswamy v. Union of India not only confirmed privacy as a fundamental right under Article 21 but also placed the concept of informational or data privacy at center stage. In the digital age, where masses of personal data are gathered, stored, and processed by state and private bodies, the Court recognized that **human autonomy and dignity would be directly linked to control over personal information.**

While the old ideas of privacy addressed physical space or personal preferences, data privacy addresses the right of an individual to control the collection, transmission, and utilization of his or her personal information, thus expanding the scope of constitutional protection to cyberspace as well as institutional records.

Aadhaar turned out to be the biggest platform in which the debate in India on data privacy took place. The program asked citizens to surrender their biometric and demographic information for authentication in financial transactions and welfare schemes, sparking concerns on surveillance, profiling, and abuse of sensitive information.

In the 2018 Puttaswamy (Aadhaar) judgment, the Supreme Court held Aadhaar to be valid but placed massive checks, for instance, preventing private entities from requiring Aadhaar-based verification. Though the judgment sought a balancing act between welfare requirements and privacy, critics contend that the presence of a biometric database remains a possible danger to personal liberty, particularly in the event of inadequate data protection measures.

ISSN: 2582-6433

10. Overview of privacy laws in india:

Prior to the promulgation of the **Digital Personal Data Protection Act, 2023**, India was without a specific legislation to address the issue of the protection of individual privacy. The issues raised in the K.S. Puttaswamy case versus the Union of India highlighted the need for the protection of individual privacy, which was repeatedly emphasized by the Supreme Court.

However, some aspects of individual privacy were protected under existing legislation. For example, under the **Indian Penal Code, 1860, Section 354C** makes voyeurism, i.e., **77 of BNS** (Bharatiya Nyaya Sanhita, 2023), a criminal offense; **Section 354D of IPC or Section 78 of BNS** makes stalking, including online stalking, a criminal offense; and **Section 228A of IPC or Section 72 of BNS** makes the disclosure of the identity of the victim of a specified offense a criminal offense.

The Information Technology Act, 2000 has been playing an important role in India in the context of data protection. Initially, it was enacted to provide legal sanctity to e- commerce and also address issues like cybercrime. However, in order to address issues like phishing, cybercrime, and other emerging technological challenges, the Act was amended in 2008. According to this Act, **Section 66A** provided for punishment for sending messages that are false, misleading, and offensive, intended to cause annoyance, inconvenience, fear, insult, injury, or hostility. Under this Act, **Sections 67 and 67A** provide for punishment for publishing or transmitting obscene and sexually explicit material, for which punishment includes seven years of imprisonment along with a fine extending to ten lakh rupees for first-time offenses and seven years of imprisonment along with a fine extending to ten lakh rupees for subsequent offenses. Furthermore, **Section 69A** provides for blocking public access to information that threatens India's sovereignty, security, and public order by direction from the Central Government.

However, in **Shreya Singhal v. Union of India**[18], the Supreme Court struck down Section 66A in its entirety for being unconstitutional and upheld Section 69A.

[18] Shreya Singhal v. Union of India, AIR 2015 SC 1523

ISSN: 2582-6433

11. Foreign Influence:

In the wake of the constitutional acknowledgment of privacy, India has proceeded to legislate the regulation of data protection. The **Personal Data Protection Bill of 2019,** which was patterned primarily after the European Union's General Data Protection Regulation **(GDPR),** aimed to adopt a rights-oriented framework and set up an independent Data Protection Authority.

The bill was, however, withdrawn in 2022, and it was later replaced with the **Digital Personal Data Protection Act, 2023.** The new law focuses on consent, purpose limitation, and accountability but has raised alarms regarding possible abuse and monitoring due to its sweeping exemptions for governmental agencies.

India's changing data privacy regime takes inspiration from international jurisprudence but grounds itself in constitutional values. It adopts concerns regarding surveillance and state interference from the United States; it learns from the European Union about integrated regulatory regimes; and it draws from its own constitutional culture in grounding privacy in dignity and personal freedom under Article 21. However, challenges remain profound. India's digital divide renders data rights hard to exercise for most of its citizens, while corporate data practices by major technology firms tend to diminish consent into a formality.

12. Some unique features of DPDP Act, 2023:

The Act defines personal data as any information that is related to an identified or identifiable individual. The Act is applicable to the processing of digital personal data in India, whether the data is collected online or offline and then converted into digital form. The Act is also applicable to data processing outside India, as long as the processing is related to the provision of goods or services in India.

Data processing in the Act is the process of carrying out fully or partly automated operations involving digital personal data, storage, utilization, and dissemination of the personal data collected. One of the most significant aspects of the Act is the **requirement of consent,** as the personal data is processed after the consent of the individual is obtained. Before obtaining the consent of the individual, a notice is issued informing the individual about the personal data being collected and the purpose of the processing of the personal data. The Act provides the

ISSN: 2582-6433

individual the option of withdrawing the consent at any time, and the consent is given on behalf of the minor by the parent or guardian.

However, the Act has provided for certain circumstances in which consent for the use is not required for legitimate uses. This includes instances in which individuals willingly provide their information for specific uses, for the dispensation of government services and benefits, in medical emergency situations, and in employment situations. In addition, the Act allows for the transfer of personal data to countries outside India, except for those that may be restricted by the Central Government.

13. Way Ahead:

The recognition of the right to privacy in India is not the culmination of a legal journey but the beginning of a continuous constitutional responsibility. While the Puttaswamy judgment marked a watershed moment by affirming privacy as a fundamental right grounded in dignity, autonomy, and liberty, the challenges of the digital era demand a forward-looking approach.

The way ahead requires the strengthening of legislative frameworks through comprehensive data protection laws modeled on global benchmarks like the GDPR, with minimal state exemptions and effective regulatory mechanisms. Equally important is judicial vigilance, where courts must consistently apply the proportionality test to balance privacy with legitimate state concerns such as national security and welfare efficiency, ensuring that vague or excessive restrictions do not dilute this right.

Encourage the development of privacy-centric technologies like end-to-end encryption and anonymisation techniques, which allow individuals and organizations to protect data without compromising usability.

At the same time, public awareness and digital literacy must be promoted so that citizens are equipped to safeguard their personal information and exercise their rights responsibly in an increasingly technology-driven society. Ultimately, privacy in the 21st century is not limited to secrecy but extends to the preservation of dignity, autonomy, and self-determination.

The evolution from Kharak Singh to Puttaswamy underscores that constitutional rights are

ISSN: 2582-6433

living instruments, capable of adapting to societal and technological transformations. As India navigates the complexities of the information age, the way ahead lies in ensuring that privacy remains both protected in law and actively preserved in practice, serving as a cornerstone of constitutional democracy.

14. References:

- M.P. Jain, *Indian Constitutional Law*, Lexis Nexis, 2013
- Radha Ranjan, *International Journal of Legal Research and Governance*, 87 (Volume 4, issue 1, march 2018)- https://www.researchgate.net/publication/371607585_RIGHT_TO_PRIVACY
- Dr. Vivek Kumar Gupta, *International Journal of Law, Justice and Jurisprudence*, 2024, (Vol. 4, Issue 1, Part C) - https://www.lawjournal.info/article/114/4-1-41-748.pdf
- Right to Privacy - Wikipedia. (2025) - https://en.wikipedia.org/w/index.php?title=Right_to_privacy&oldid=1308060594
- https://vajiramandravi.com/upsc-exam/right-to-privacy/