
PRIVACY AS A FUNDAMENTAL RIGHT: IMPACT AND IMPLEMENTATION AFTER PUTTASWAMY

Rohit Raikwar, B.B.A LL.B. (Hons.), Mediacaps University, Department of Law, Indore,
Madhya Pradesh

ABSTRACT

The “Right to Privacy” was recognized as a Fundamental Right in Justice. K.S. Puttaswamy (Retd.) v. Union of India (2017)¹ marking a historic moment in Indian constitutional law. However, the transition from official declaration to real implementation has not been smooth. After this historic ruling, which rejected previous restrictive interpretation and created a strong foundation for future privacy claims under Articles 14, 19, and 21 of the constitution, this essay critically examines how India's privacy jurisprudence has evolved. The supreme court developed a robust three part- test legality, legitimate intent and proportionality to access any official breach of privacy.

Building on these concepts the report looks at how subsequent supreme court rulings expanded and applied the right to privacy in a variety of contexts, including digital access, corporate data practices, marital privacy, and the use of biometric data.(Aadhaar)

Furthermore, the report evaluates the legislative response, particularly the enactment of the Digital personal Data protection Act, 2023. and its adequacy in addressing emerging privacy concerns. In its conclusion, it emphasizes how crucial the judiciary is in preserving personal freedom and dignity in an increasingly data-driven world.

Through a doctrinal and analytical approach, this study emphasizes the evolving and dynamic nature of privacy rights in India. It argues for stronger institutional safeguards, informed judicial oversight, and public accountability to uphold the spirit of Puttaswamy in the face of rapid technological and societal changes.

Keywords: Right to Privacy, Puttaswamy Judgment, Indian Constitutional Law, Informational Privacy, Proportionality Test

¹ Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1

I. PREFACE

As someone from the Gen Z generation, I've observed how casually we share our personal information online, often without considering where it goes or how secure it is. From AI tools and websites to verification systems and government schemes, we give up data without questioning the implications. What concerned me even more was how this casual disregard extends into real life, where people are investigated, searched, or profiled with little regard for their privacy.

These everyday concerns sparked my interest in understanding the legal protections around privacy in India. The landmark *Justice K.S. Puttaswamy V. Union of India* judgment became the starting point for my research, as it recognized privacy not just as a legal right, but as a cornerstone of dignity and autonomy.

This paper explores how the right to privacy has evolved in Indian jurisprudence after the Puttaswamy decision-especially in light of digital challenges, surveillance, and the growing power of private tech platforms. What began as a personal concern became a deeper legal inquiry into how far our constitutional safeguards truly extend.

II. INTRODUCTION

A. Background

The concept of privacy in India has long existed in legal grey zone, widely experienced in personal life but absent from explicit constitutional recognition for decades. For a country like India, with its diverse social fabric and deep rooted administrative practices, the evolution of privacy as a legal right was gradual, marked by ambiguity, contradictions, and finally a turn point in 2017. Early Judicial ruling, notably *M.P Sharma v. Satish Chandra (1954)*² and *Kharak singh v. State of Uttarpradesh (1962)*³, denied privacy the status of protected right, largely due to a narrow interpretation of constitutional text, However, as the interpretation of Article 21 evolved, the Supreme Court began to expand the scope of 'personal liberty' to encompass newer dimensions such as dignity, autonomy, and bodily integrity.

² M.P. Sharma v. Satish Chandra, AIR 1954 SC 300

³ Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295

This evolving jurisprudence reached its constitutional zenith in *Justice K.S. Puttaswamy (Retd.) V. Union of India* (2017), where a nine-judge bench of the Supreme Court unanimously affirmed that privacy is an inherent inalienable fundamental right under PART III of the constitution. The court declared that privacy is not only intrinsic to Article 21⁴ but also interlinked with **Articles 14⁵ and 19⁶**, thereby placing it within the heart of India's constitutional identity. The judgment dismantled outdated precedents and introduced a nuanced, multidimensional understanding of privacy, setting the stage for future legal reforms and judicial interventions.

B. Legal Precedents Leading To The judgment

Historically, the Indian government maintained that the Constitution did not explicitly guarantee a right to privacy. This position was bolstered by earlier Supreme Court judgment, notably.

1. *M.P Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962) - *The Denial Phase*, In *M.P Sharma* case, an eight-judge bench held that the Indian Constitution did not recognize a right to privacy. This was reiterated in *Kharak Singh V. State of U.P*, where the majority refused to acknowledge privacy as a constitutional guarantee, though a powerful dissenting opinion by Subba Rao, J., laid the groundwork for future expansion.

2. *Gobind v. State of M.P* (1975)⁷, *People's Union for Civil Liberties v. Union of India* (PUCL)⁸, - *Emergence of a Qualified Privacy Rights*, Due to conflicting rulings from benches with varying degrees of strength, this resulted in a jurisprudential conflict that required a final ruling from a larger bench in order to authoritatively decide the privacy status. In order to address this crucial constitutional issue, a nine-judge bench was established.

3. **Pre Puttaswamy Fragmentation:-** Following *Gobind*, several cases engaged with specific dimensions of privacy but stopped short of general recognition. In *PUCL V. Union of India*, the court recognized privacy interests in the context of telephone tapping, but even these judgments

⁴ Art. 21, The Constitution of India, 1950

⁵ Art. 14, The Constitution of India, 1950.

⁶ Art. 19, The Constitution of India, 1950

⁷ *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148

⁸ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301

treated privacy as fragmented, linked to specific factual contexts rather than as a general constitutional guarantee.

A transformative shift occurred with *Maneka Gandhi V. Union of India (1978)*⁹, where the Supreme Court dramatically expanded the interpretation of Article 21 by introducing the doctrine of “substantive due process.” The court held that any law infringing personal liberty must be just, fair, and reasonable, not merely backed by legislation. This landmark ruling marked a critical inflection point in Indian Constitutional law, laying the groundwork for recognizing privacy as essential to a life of dignity, autonomy, and freedom.

C. Scope And Methodology

This paper seeks to critically analyze the judicial journey of the Right to Privacy in India after the *Puttaswamy* judgment. It Focuses on the application of privacy principles in key post-2017 cases, especially those that address areas such as digital surveillance, state-led biometric identification, sexual autonomy and private sector data practices.

The scope includes FIVE significant Supreme Court decisions:

1. *Puttaswamy II (Aadhaar judgment)* - Informational privacy and proportionality
2. *Navtej Singh Johar* - Sexual orientation and decisional autonomy
3. *Joseph Shine* - Gender equality and marital privacy
4. *Anuradha Bhasin* - Digital rights and internet shutdowns
5. *Karmanya Singh Sareen (WhatsApp Privacy Case)* - Informational vs. Corporate Data use

The methodology adopted is doctrinal, grounded in the analysis of constitutional texts, judicial opinions, and interpretative trends. Supplementary insights are drawn from policy documents, scholarly commentary and development such as the Digital Personal Data Protection Act, 2023. Rather than offering a purely theoretical view, this study attempts to evaluate how privacy is evolving in real-world legal contexts, particularly for today’s technology-dependent, data

⁹ *Maneka Gandhi v. Union of India*, AIR 1978 SC 597 AIR 1978 SC 597

sharing generation.

III. The Puttaswamy judgment: A landmark Shift

A. Fact of the case

The constitutional journey of the right to privacy in India reached its turning point with the landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, decided on 24 August 2017 by a nine-judge bench of the Supreme Court. The genesis of this case stemmed from a legal challenge against the Aadhaar scheme, initiated by the Government of India. The petitioners, led by former High Court Judge Justice K.S. Puttaswamy, argue that the mandatory collection of biometric data-fingerprints, iris scans, and demographic information, without a comprehensive legal framework infringed upon the fundamental right to privacy. Initially brought before a three-judge bench, the case was referred to a larger constitutional bench due to conflicting precedents from earlier ruling in *M.P. Sharma V. Satish Chandra (1954)* and *Kharak Singh V. State of U.P) (1962)*, which had held that privacy was not a fundamental right under the Constitution. Recognizing the constitutional significance, a rare nine-judge bench was constituted to determine the broader question: Whether the right to privacy is a fundamental right under the Indian Constitution.

B. Key Legal Questions Addressed

The case did not solely revolve around the Aadhaar scheme. It posed foundational constitutional questions that had implication across all domains of law and governance. The core legal questions were:

1. Whether the Constitution of India guarantees a fundamental right to privacy under Part III.
2. If so, is it a standalone right or embedded within existing rights like Article 21?
3. What are the doctrinal foundations of privacy within constitutional jurisprudence
4. What is the scope of content of privacy as a right?
5. What are the limits of state power to regulate or curtail this right?

These question necessitated a comprehensive judicial interpretation of the Constitution, leading to the formulation of new doctrinal standards.

C. Majority Opinion and Key Observation

The bench unanimously held that the right to privacy is a fundamental, inalienable, and intrinsic right under Part III of the Constitution, specifically arising from Articles 14, 19, and 21.

Key observation Included:

1. Privacy encompasses bodily integrity, informational privacy, and decisional autonomy.
2. It is not elitist right but applicable to all individuals regardless of class or status.
3. The court introduced a three-fold test to determine valid restrictions on privacy:

A. **Legality** - The restriction must be backed by law

B. **Legitimate Aim** - The state must pursue a constitutionally valid objective.

C. **Proportionality** - The means adopted must be necessary and the least intrusive.

D. Overruling of Previous Jurisprudence

The court explicitly overruled *M.P Sharma and Kharak Singh* to the extend that they denied the existence of a fundamental right to privacy. It emphasized the Constitution as a living document and rejected the idea that silence on privacy in the Constitution amounted to denial. According to Chandrachud, J.'s concurring opinion, "Privacy is the constitutional core of human dignity.

E. Constitutional Status of Privacy Post-Judgement

After Ruling, privacy became constitutionally protected under Article 21, with implication across all fundamental rights in Part III. It was recognised as:

- An Inherent and inalienable natural right.
- Essential to the enjoyment of all other Freedoms (speech, movement, association).

- Subject to reasonable limitations, similar to other fundamental rights.

The Court clarified that privacy is not a standalone right but one that animated and strengthens existing constitutional guarantees.

F. Expansion into other Domains

There have been impacts from the acceptance of privacy as a safeguard against government interference as well as supporter of individual choice. Future decisions like *Navtej Singh Johar V. Union of India (2018)*¹⁰ (decriminalizing homosexuality) and *Joseph Shine V. Union of India (2019)*¹¹ (decriminalizing adultery) expanded on reproductive rights, personal choices, and dignity after informational privacy and decisional autonomy were given constitutional status. Additionally, the ruling's focus on appropriate and legal state action has influenced constitutional analysis in cases involving digital restrictions and surveillance. The Supreme Court upheld online freedom of expression and digital privacy in *Anuradha Bhasin V. Union of India (2020)*¹² by using the three fold proportionality test to access the legality of internet shutdowns.

IV. The Post-Puttaswamy Era: Impact of the Judgment

The *Justice K.S. Puttaswamy v. Union of India (2017)* judgment fundamentally reshaped Indian constitutional law by affirming the right to privacy as a fundamental right under Article 14, 19, and 21. It established a structured three-fold proportionality test, requiring legality, a legitimate state aim, and necessity, now applied across diverse privacy contexts. The following landmark cases illustrate how courts have operationalized *Puttaswamy's* principles in varied domains.

1. Informational Privacy and Biometric Data

Case:- *Justice K.S. Puttaswamy (Aadhaar) v. Union of India, (2019)*¹³

1.1 Context

The Aadhaar Act, 2016 introduced a system where every Indian could be identified through

¹⁰ Navtej Singh Johar v. Union of India, (2018) 10 SCC 1

¹¹ Joseph Shine v. Union of India, (2019) 3 SCC 39

¹² Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

¹³ Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1

biometric details (Fingerprints, iris scan) and basic demographic data to access government welfare schemes. While the aim was to reduce corruption and ensure subsidies reached the right people, critics argued it created a risk of surveillance, misuse of personal data, and loss of privacy especially if the data was centralized or shared without consent.

1.2 How court Applied the Puttaswamy Proportionality Test:

1. Legality: The court found that Aadhaar had a clear legal basis because it was backed by the Aadhaar Act.

2. Legitimate State Aim: The main goal, ensuring subsidies reached only genuine beneficiaries - was considered legitimate.

3. Necessity & Proportionality: The court held that collecting only minimal details (name, address, biometrics) was proportionate for welfare purposes, but provisions enabling private sector use, mandatory linking with bank accounts and SIM cards, and excessive data retention failed the test.

1.3 Impact

In a 4:1 majority, the court upheld Aadhaar for welfare purposes but struck down provisions inconsistent with proportionality:

- **Section 57¹⁴:** Private Companies can no longer demand Aadhaar authentication.
- **Section 33(2)¹⁵:** Removed the vague “national security” clause that allowed Aadhaar data to be shared without any court oversight.
- **Regulation 27¹⁶:** Personal Data can be kept for only six months (earlier to could be stored for five years).
- **Upheld:** Aadhaar- PAN linking for tax purposes was kept, as it was seen as proportionate for preventing tax fraud.

¹⁴ § 57, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

¹⁵ § 33(2), The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

¹⁶ Reg. 27, The Aadhaar (Authentication) Regulations, 2016.

2. Decisional Autonomy and Sexual Freedom

*Case: Navtej Singh Johar v. Union of India, (2018)*¹⁷

2.1 Context

This case Challenged Section 377 IPC¹⁸, which criminalized consensual homosexual acts. The petitioners argued that it violated the rights to privacy, dignity, and equality, relying heavily on *Puttaswamy (2017)*. The earlier *Suresh Koushal*¹⁹ ruling, which upheld the provision on the ground that it affected only a “minuscule fraction” of the population, was directly questioned.

2.2 Application of Puttaswamy Principles:

1. **Sexual Orientation as Part of Identity** - The Court, drawing from *Puttaswamy*, recognized sexual orientation as an intrinsic part of self-identity. Denying this right would infringe on privacy and dignity under Article 21.
2. **Constitutional morality over popular morality** - Building on *Puttaswamy*'s rejection of majoritarian views, the Court clarified that constitutional morality, not public opinion, determines the scope of fundamental rights.
3. **Freedom of Expression** - Criminalizing consensual homosexual acts was seen as an unreasonable restriction on free speech under Article 19(1)(a), as it prevented individuals from openly expressing their sexual identity.
4. **Decisional Autonomy**: It held that privacy is not limited to being left alone but includes decisional autonomy, the freedom to make intimate personal choices without state interference.

2.3 Impact

1. **Decriminalization** - Consensual Homosexual acts between adults in private were decriminalized.
2. **Overruling Suresh Koushal** - Rejected the “minuscule fraction” argument, affirming that

¹⁷ Navtej Singh Johar v. Union of India, (2018) 10 SCC 1

¹⁸ § 377, The Indian Penal Code, 1860.

¹⁹ Suresh Kumar Koushal v. Naz Foundation, Civil Appeal No. 10972 of 2013 (Supreme Court of India, December 11, 2013).

rights are universal.

3. Strengthening LGBTQ+ Rights - Provided a strong constitutional foundation for future legal and social reforms.

4. Social Change - Catalyzed public awareness, acceptance, and visibility for LGBTQ+ communities.

3. Gender Equality and Marital Privacy

*Case: Joseph Shine V. Union of India, (2019)*²⁰

3.1 Context

Section 497 of the Indian Penal Code, a 150 Year old colonial provision, criminalized adultery, treating women as the property of their husbands and denying them equal agency. Only husbands could prosecute, reflecting colonial-era patriarchy reinforced by section 198(2) CrPc.

3.2 Application of Puttaswamy Principles:

1. Legality - Although backed by statute, the law failed constitutional tests under Articles 14, 15, and 21 for being arbitrary and discriminatory.

2. Necessity & Proportionality - Criminalizing adultery was unnecessary when civil remedies like divorce were sufficient. Adultery was reclassified as a private wrong, not a criminal offence.

3. Privacy and Autonomy in Marriage - The court held that marriage does not erase individual dignity or decisional autonomy. The right to choose an intimate partner falls within a person's sexual and decisional privacy.

4. Equality in Marital Relationships - Privacy cannot be misused to shield gender inequality; marriage is a partnership between equals.

²⁰ Joseph Shine v. Union of India, (2019) 3 SCC 39.

3.3 Impact

1. Striking Down of Section 497 of the IPC and Section 198(2) of the CrPC - Both provisions were declared unconstitutional, removing criminal liability for adultery.

2. Advancement of Gender Equality - The decision dismantled a colonial-era, male-centric legal structure and affirmed that women have equal status and agency within marriage.

3. Recognition of Marital Privacy - Extended privacy protections into marital life, ensuring dignity within domestic relationships.

4. Shift in Social Understanding - Recognized marriage as a partnership based on equality, dignity, and mutual respect, rather than ownership and control.

4. Corporate Data Practices and Informational Self- Determination

*Case: Karmanya Singh Sareen v. Union of India, (2017)*²¹

4.1 Context

In 2016, Whatsapp changed its privacy policy to allow sharing of user data, including phone numbers and usage patterns, with its parent company, Facebook. This raised serious concerns about how private tech companies handle massive amounts of personal data, and whether individuals have real control over how their information is used.

The petitioners argued that users had joined whatsapp under its earlier policy, which promised strong privacy protection, and that the sudden change violated their rights to privacy. The case, while still pending, played a crucial role in highlighting the need for statutory protection against the misuse of personal data by private corporations. It was a key legal driver behind the creation of the Digital Personal Data Protection Act, 2023, by reinforcing the principles established in the *Puttaswamy* judgment and underscoring the horizontal application of privacy rights.

4.2 Application of Puttaswamy Principles:

1. Informational Privacy: - Puttaswamy recognized that people have the right to control their

²¹ Karmanya Singh Sareen v. Union of India, (2017) 8 SCC 291

personal data. The policy change forcing data sharing with Facebook was argued to violate this right.

2. Horizontal Reach - It acknowledged that privacy can also apply to private entities, especially when they control essential services like WhatsApp.

3. Necessity & Proportionality- The data sharing was neither essential for WhatsApp's core service nor proportionate, and it lacked proper consent safeguards.

4. Need for a Data Law - *Puttaswamy* had called for a strong data protection law, and this case reinforced that need, leading to the Digital Personal Data Protection Act, 2023

4.3 Impact

1. Pushed for a New Data Protection Law - This case helped speed up the creation of the Digital Personal Data Protection Act, 2023, which now controls how both the government and private companies handle people's personal information.

2. Involvement of Multiple Regulators - Apart from the Supreme Court, the Competition Commission of India (CCI) also stepped in to check if WhatsApp was misusing its dominant position, show that privacy issues can connect with competition law.

3. Greater Public Awareness - The case made more people aware of how tech companies collect and share their data, and why clear rules and proper consent are important.

4. A test for Digital Rights in India - It has become an important example for deciding how India will protect people's rights in the digital age, especially against big technology companies.

V. The Implementation of Puttaswamy Principles

A. Legislative Implementation - The Digital Personal Data Protection Act, 2023

1. Journey from the Judgment to Law

After the *Puttaswamy* (2017) judgment, the Supreme Court stressed the need for a clear privacy law. The government set up the Justice B.N. Srikrishna Committee in 2017, which proposed a

rights-based data protection framework. The committee's report in 2019 was Titled "*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indian*"²².

Following the report, the Personal Data Protection Bill, 2019 was introduced in parliament, but it faced multiple criticism, and concerns over excessive government powers delayed its passage. The original bill was withdrawn in 2022. The government then introduced the Digital Personal Data Protection Bill, 2023, which was passed by both Houses of Parliament, and received Presidential assent in August 2023 as the "Digital Personal Data Protection Act, 2023 (DPDP Act).

This Legislative journey was also influenced by ongoing privacy litigations, most notably "*Karmanya Singh Sareen v. Union of India (WhatsApp Privacy Case, 2017)*", which highlighted the urgent need for statutory protection against misuse of personal data by both state and privacy sectors.

2. Key Provisions of DPDP Act

The Digital Personal Data Protection Act, 2023 is India's first dedicated privacy law and reflects several principles from *Puttaswamy case* (2017), such as consent-based data processing, purpose limitation, and security safeguards. These provisions align with the judgment's emphasis on autonomy, proportionality, and protection from arbitrary interference.

Key Provisions:

1. Consent Based Processing - Data can be collected and processed only with the user's free, informed, and revocable consent, except in certain legitimate uses.
2. Purpose Limitation - Data must be used only for specific purposes for which it was collected.
3. Rights of Data Principals - Includes the right to access information, correct or erase personal data, and nominate representatives in case of incapacity or death.
4. Duties of Data Fiduciaries - Entities handling data must ensure accuracy, security, and timely breach reporting.

²² B. N. Srikrishna Committee, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2019)

5. Data Protection Board - Established to enforce compliance and adjudicate violations.

3. Critical Analysis

Strengths -

1. Aligns with *Puttaswamy* by embedding consent, necessity, and proportionality.
2. Applies to state and private entities.
3. Empowers users through defined rights.
4. Mandates security Safeguards and breach reporting.

Weaknesses -

1. Broad government exemption for “national security” and “public order”
2. Data Protection Board lacks Independence
3. Limited Rights Compared to global standards (e.g. GDPR).
4. Unclear enforcement against powerful tech companies.

Overall Assessment

The DPDP Act is foundational milestone in India’s privacy journey. It codifies core privacy principles, establishes a dedicated regulatory body, and extends protections to both state and private sectors. However, loopholes in exemption, limited regulator independence and narrower user rights dilute its potential. For it to fully embody the spirit of *Puttaswamy*, Future reforms must narrow state powers, strengthen the regulator, and expand individual rights in line with global test practices.

B. Judicial Enforcement

Courts have actively applied *Puttaswamy* to protect privacy in various Context:

1. *Puttaswamy II (Aadhaar Judgment, 2018)* - Applied the proportionality test; upheld Aadhaar

for Welfare schemes but struck down provisions enabling excessive data collection and private use.

2. *Navtej Singh Johar v. Union of India (2019)* - Decriminalised consensual homosexual acts; expanded decisional autonomy.

3. *Joseph Shine v. Union of India (2020)* - Struck down adultery law for violating dignity and autonomy.

4. *Anuradha Bhasin v. Union of India (2020)* - Applied proportionality to internet shutdowns; reinforced digital privacy.

5. *Pegasus Surveillance Case (2021)* - Supreme Court Formed an independent technical committee, recognizing privacy as shield against mass surveillance.

These cases show That implementation has not been confined to legislation, the judiciary continues to develop privacy jurisprudence through active constitutional interpretation.

C. Institutional and Policy Reforms

1. Regulatory Bodies - Creation of the Data Protection Board to enforce the DPDP Act.
2. Sectoral Guidelines - Health, telecom, and banking regulators issuing privacy compliance rules.
3. Government Protocols - New norms for secure storage, processing, and sharing of citizen data.
4. Inter-Agency Coordination - Greater involvement of the Competition Commission of India in cases like the *WhatsApp Privacy Policy Dispute*, addressing abuse of dominant position alongside privacy concerns.

D. Practical Challenges

1. Public Awareness - Citizens, especially younger generations, remain unaware of their privacy rights.
2. Technical Gaps - Many institutions lack infrastructure for compliance.

3. Balancing Interests - Ongoing tension between privacy and state security goals.
4. Enforcement Capacity - The effectiveness of Data protection Board remains untested.

VI. Conclusion

From its uncertain beginning in *M.P. Sharma* and *Kharak Singh*, where privacy was denied constitutional recognition, to its emphatic affirmation in *Justice K.S. Puttaswamy v. Union of India* (2017), the right to privacy in India has undergone remarkable transformation. The jurisprudential journey from fragmented protection in cases like *Gobind* and *PUCL* to the doctrinal leap in *Maneka Gandhi* laid the foundation for *Puttaswamy*'s multidimensional understanding of privacy as intrinsic to dignity autonomy and liberty under Articles 14, 19, and 21.

The post-*Puttaswamy* era has witnessed privacy shaping key constitutional developments, whether in *Navtej Singh Johar* (Sexual autonomy), *Joseph Shine* (gender equality), *Anuradha Bhasin* (digital freedoms), or the ongoing *Karmanya Singh Sareen* case (corporate data practices). The legislative culmination in the Digital Personal Data Protection Act, 2023 represents progress but also reveals critical shortcomings, particularly in its broad state exemptions and regulatory independence.

The *Puttaswamy* judgment was not the final word but the starting point of an evolving constitutional narrative. To truly realize its promise, India must refine its legislative framework, strengthen independent oversight, and foster digital literacy so that privacy protections match the realities of rapidly changing technological and social landscape. Just as the introduction traced privacy's uncertain origins to its constitutional recognition, this conclusion reaffirms that its future will depend on a sustained commitment to the principles of dignity, autonomy and freedom that *Puttaswamy* placed at the heart of India's constitutional Identity.

REFERENCES (ILI Style)

Case Laws:-

- *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637
- *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148
- *Justice K.S. Puttaswamy (Retd.) and Anr v. Union of India and Ors*, (2017) 10 SCC 1
- *Joseph Shine v. Union of India*, (2019) 3 SCC 39
- *Karmauya Singh Sareen v. Union of India*, (2017) 8 SCC 291
- *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295
- *Maneka Gandhi v. Union of India*, AIR 1978 SC 597
- *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300
- *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1
- *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301
- *Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1
- *Suresh Kumar Koushal v. Naz Foundation*, Civil Appeal No. 10972 of 2013, Supreme Court of India, Dec. 11, 2013

Statutes:-

- Regulation 27, The Aadhaar (Authentication) Regulations, 2016
- §57, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
- §33(2), The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

- §377, The Indian Penal Code, 1860

The Constitution of India, 1950:-

- Art. 14, The Constitution of India, 1950
- Art. 19, The Constitution of India, 1950
- Art. 21, The Constitution of India, 1950

III. Books & Articles:-

- Aashna Jindal, “Right to Privacy as a Fundamental Right in India: Evolution, Challenges and the Impact of Digitalization,” 6 Int’l J. Multidisciplinary Res. 6 (2024).
- Padmanabhan, “Right to Privacy as an Implied Fundamental Right – An Analysis,” in *Anthology on Law and Privacy* (INSC International Publishers 2021).
- Rituparna Panigrahi & Archana Mehta, “The Impact of the Puttaswamy Judgement on Law Relating to Searches,” 15 NUJS L. Rev. 1 (2022).

Reports:-

- B. N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 2019