

LEGAL LOCK JOURNAL

2583-0384

VOLUME 4 || ISSUE 3

2025

This Article is brought to you for “free” and “open access” by the Legal Lock Journal. It has been accepted for inclusion in the Journal after due review.

To submit your Manuscript for Publication at Legal Lock Journal, kindly email your Manuscript at legallockjournal@gmail.com.

THE EVOLUTION OF RIGHT TO PRIVACY IN INDIA: A SOCIO-LEGAL APPROACH

Devansh Tripathi¹ & Dr. Anuj Kumar Sharma²

ABSTRACT

The jurisprudential path of the right to privacy in India is a rich constitutional transformation—both from an implicit, formless notion to a categorically enshrined fundamental right. Rooted in a colonial legacy of intrusive surveillance, the evolution of privacy jurisprudence reflects a dynamic interplay between judicial interpretation, civil liberties, and the imperatives of a rapidly digitising society. This paper critically examines seminal judicial pronouncements, from the tentative recognition in *Kharak Singh v. State of Uttar Pradesh* to the watershed moment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, wherein privacy was considered to be included in the right of life and liberty of an individual under Article 21. By tracing the doctrinal shifts and contextualising them within contemporary challenges such as data surveillance, biometric identification, and algorithmic governance, this study underscores privacy's transition from a peripheral legal construct to a cornerstone of democratic ethos and human dignity in the Indian constitutional framework.

¹ The author is a student of law at Amity Law School, Lucknow.

² The Co-Author is a professor of law at Amity Law School, Lucknow.

1. INTRODUCTION

1.1 General Introduction

Though not enumerated as such in the wording of the original Indian Constitution, the right to privacy has now become part and parcel of the right to life and liberty under Article 21. The Indian judiciary has interpreted the Constitution step by step to recognize and protect a vast array of human freedoms, with privacy now holding a particularly significant place. It covers many facets of the human experience, including decision-making freedom, data protection, and physical and physiological autonomy. In contemporary constitutional jurisprudence, the notion that people ought to have authority over the information they reveal, The significance of the choices individuals make and the legal threats they can repel has increased.

In the landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-judge bench of the Supreme Court held privacy to be a fundamental right that is essential to equality, liberty, and dignity, bringing this recognition to the level of constitutional maturity. The ruling overturned previous rulings and reinterpreted the constitution in light of evolving legal, technical, and sociological trends. The right to privacy is today seen as crucial to maintaining individual autonomy and defending democracy itself in a world when digital platforms, ubiquitous data gathering, governmental monitoring, and biometric identity systems like Aadhaar are the norm.

1.2 Research Objectives

- To discuss the development of the right to privacy by Indian courts.
- To evaluate the impact of landmark constitutional cases.
- To compare India's privacy policy with international standards.
- To suggest legal reforms for better protection of privacy.

1.3 Review of Literature

Legal theorists and academics have long been fascinated by the idea of privacy. The theoretical foundation was laid by Alan Westin's early work, which defined privacy as a way for individuals to have control over the sharing of their information. Post-Puttaswamy literature has significantly grown in the Indian setting. Researchers have

looked at privacy from a number of angles, including intersectional discrimination, digital surveillance methods, biometric data gathering (Aadhaar), and right to be forgotten. Lack of robust data protection legislation in India and piecemeal judicial protection in certain regions have also been the matter of legal grievances.

The struggle between competing constitutional rights, e.g., freedom of speech and the right to knowledge and privacy is systematically depicted in literature. The development of the topic of digital rights has further influenced privacy discussions, especially those pertaining to algorithmic transparency, tech firm responsibility, and government control of online activity.

1.4 Research Design

This study uses a doctrinal approach, drawing on international legal instruments, case law analysis, and constitutional interpretation. It places the evolution of this right amid larger socio- political and legal changes by charting the historical development of privacy jurisprudence in India. Comparative viewpoints with other legal systems, such as the US and the EU, provide information on possible reform frameworks. The goal of the study is to examine privacy as a lived and socially created right that is impacted by changing governance paradigms and technological advancements, rather than only as a legal abstraction.

2. RIGHT TO PRIVACY IN INDIA

2.1 New Perspective on Article 21

Article 21 of the Constitution of India says that “no person shall be deprived of his life or personal liberty except according to procedure established by law.”³ The Supreme Court adopted a limited view in early instances such as *A.K. Gopalan v. State of Madras*, equating "procedure established by law" with any lawfully passed laws, regardless of its fairness.⁴ The Court in *Maneka Gandhi v. Union of India*, broadened Article 21 to incorporate the concepts of justice, rationality, and non-arbitrariness, which marked the

³ INDIA CONST. art. 21.

⁴ *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.

beginning of a shift in this strategy.⁵ This transformation laid the foundation for reading unenumerated rights, such as privacy into the Constitution.

2.2 Right Against Surveillance

In democratic democracies, surveillance, especially by state officials, has sparked grave constitutional concerns. From internet monitoring and phone tapping to biometric tracking and face recognition, the spread of surveillance technologies in India has surpassed the legislative measures intended to control them. The Supreme Court considered whether tapping of telephones by the state was legal in the landmark case of *People's Union for Civil Liberties v. Union of India (PUCL)*. In line with the Court's consideration of the practice pursuant to Article 21, any monitoring constitutes a serious encroachment on the right to privacy of an individual. According to the ruling, such monitoring can only be appropriate if it passes the combined legality, need, and proportionality standards.⁶ These criteria require that the surveillance must be backed by a valid law, meant to serve a valid governmental objective, and to utilize the least intrusive means available. This ruling made clear that unapproved surveillance is unlawful, particularly in the absence of legal protections.

The Court established comprehensive procedural protections to operationalise these principles. These include regular reviews by a designated oversight committee, appropriate recording of the reasons for interception, and obligatory prior clearance by a high-ranking official, such as the Home Secretary. These precautions were put in place to guard against abuse, shield against capricious intrusions, and encourage accountability and openness in state monitoring systems. The PUCL instructions need to be codified into legally enforceable legislation immediately since, in reality, numerous surveillance acts still take place without sufficient checks or transparency, despite these directives, according to further investigations.

2.3 Right to Protect One's Own Privacy

In *R. Rajagopal v. State of Tamil Nadu*, the Supreme Court dealt with the issue of unauthorized publication of a convict's autobiography by a magazine, which raised crucial

⁵ *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

⁶ *People's Union for Civil Liberties v. Union of India*, AIR 1997 SC 568.

concerns around media intrusion and the limits of press freedom.⁷ The Court determined that everyone is entitled to privacy, including the right not to have personal facts published without consent, even when the facts are true. This was a historical decision in the sense that it stated that the right to privacy of an individual is not breached merely because facts are public knowledge or in the public domain; instead, the issue is whether they have given or not given consent.

The Court noted an important distinction between information pertaining to an individual's private life and information pertaining to official behaviour or public obligations, the latter of which are subject to public scrutiny. By stating that journalistic freedom does not grant unrestricted access to private life, the Court tried to balance, at the constitutional level, between freedom of the press according to Article 19(1)(a) and privacy of the person according to Article 21. The principle of informational self-determination, which holds that people should have choice over how their personal information is used and disseminated, was first articulated in India with this verdict.

In essence, *Rajagopal* was essentially a forerunner of current discussions about digital doxxing, media sensationalism, paparazzi culture, and data protection. In the framework of freedom of expression, it cleared the path for a more nuanced judicial understanding of personal autonomy. It is still cited in situations concerning defamation, publishing prohibitions, and public figures' rights to privacy protection.

2.4 Protection of Identity of Rape Victims

The Indian Penal Code's Section 228A expressly makes it illegal to reveal a rape victim's identity, demonstrating the legislature's intention to shield victims from additional suffering and social disgrace. The clause guarantees the confidentiality of the victim's name or any information that may be used to identify them and is applicable to the media, law enforcement, and even private citizens. The broader constitutional right of privacy and dignity under Article 21 forms the basis of this statutory protection as well as the language of the statute. The Supreme Court reaffirmed the necessity of anonymity of victims of sexual abuse in the case of *State of Punjab v. Ramdev Singh*.⁸ The Court underlined that protecting a rape survivor's identity is a substantive right that preserves the person's dignity, autonomy, and mental health rather than only being a procedural one. It noted

⁷ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

⁸ *State of Punjab v. Ramdev Singh*, AIR 2004 SC 1290.

that revealing the identification can result in mental pain, social exclusion, and further victimisation. The ruling unequivocally confirmed that in certain situations, privacy goes beyond informational control and becomes crucial for individual safety and reintegration into society.

Through the requirement that pseudonyms such as "X," "Y," or "Miss A" be used in court orders and media coverage, Indian courts have further strengthened these safeguards. This idea is also supported by directives from the Ministry of Information and Broadcasting and guidelines published by the Press Council of India. These steps are intended to prevent victims from experiencing ongoing trauma as a result of public exposure. Furthermore, these safeguards support the notion that the right to privacy extends beyond informational confidentiality and is a prerequisite for dignity, especially for marginalised or vulnerable people.

2.5 Telephonic Surveillance

Reinforcing PUCL, the Court has repeatedly affirmed that conversations over the telephone even in public are protected by privacy rights.⁹ Debates over illegal eavesdropping have been rekindled by the rise of spyware programs like Pegasus, highlighting the need for improved technology protections and legislative changes. However, this long-standing legal framework is now facing fresh issues due to the rise of spyware technology, especially programs like Pegasus. Debates concerning the boundaries of legal eavesdropping have been rekindled by Pegasus, a powerful spying tool that can monitor locations, intercept phone calls, and access private messages without the user's knowledge.

2.6 Intersection with Freedom of Speech

Legal theory has long been concerned with how to balance free speech and privacy. The Indian Supreme Court reiterated in the historic judgment of *Rajagopal v. State of Tamil Nadu* that officials of the public cannot invoke the right to privacy as a defense to avoid public scrutiny of their official conduct.¹⁰ The judgment made the valuable distinction between the right to privacy of an individual and the right of the public to know how persons in authority act. The Court's ruling was premised on the fact that, because public officials occupy positions that have an impact on the well-being of the community, their

⁹ *PUCL*, AIR 1997 SC 568.

¹⁰ *R. Rajagopal*, (1994) 6 SCC 632.

acts need to be subject to public debate and examination.

Although the Court acknowledged the need of openness in public officials' operations, it also made clear that the right to privacy still applies when it comes to private information unconnected to one's public position. The right to privacy still protects personal information that has nothing to do with governmental actions or the general welfare. This differentiation allows persons, even if they are well-known, to also retain some form of privacy in their private lives without facing possible or undue exposure to the general public.

2.7 Emergency and Privacy

India's Emergency (1975–77) was characterised by extensive abuses of authority, including infringements on fundamental freedoms and rights. Basic rights such as the right to privacy and personal liberty were drastically during this time, frequently in the interests of national security. These violations brought to light the constitutional framework's weaknesses and the necessity of more robust protections to uphold basic rights even during emergencies.

The 44th Constitutional Amendment Act of 1978 was passed in reaction to the executive branch's abuse of authority during the Emergency. Articles 20 and 21—concerning protection against arbitrary arrest and detention and protection of life and personal liberty, respectively—were strengthened as a result of this amendment, which significantly altered the Constitution. The amendment made it clear that in the event of a national emergency, these rights could not be suspended or altered.¹¹

This was essential because it reasserted that right of privacy that forms a fundamental aspect of right to life and personal freedom granted under Article 21, would continue to be maintained even in emergency situations or other extraordinary situations. Prior to this amendment, there had been concerns that, as in the Emergency period, the government would ignore some fundamental rights in times of emergency. The 44th Amendment created a permanent constitutional safeguard against executive overreach by making Articles 20 and 21 non-derogable. This made it impossible to compromise the protection of privacy and individual liberty, even in the event of emergencies or national security concerns.

¹¹ The Constitution (Forty-Fourth Amendment) Act, 1978.

The view that there are some freedoms of individuals, including privacy, that are essential to constitutional coherence and must be upheld even in the most extraordinary situations has been reinforced by this protection, which has had a long-lasting effect on how constitutional rights are interpreted in India.

3. JUDICIAL STANDPOINT ON RIGHT TO PRIVACY IN INDIA

In *M.P. Sharma v. Satish Chandra* (1954), the Indian Supreme Court had to rule on the question of privacy and held that the Indian Constitution does not provide a general right of privacy.¹² The question before them was whether searches and seizures made under the Criminal Procedure Code were legal or not. The Court ruled that no broad, inalienable right of privacy was included in the constitutional fundamental rights, particularly under Articles 19 and 21. The ruling effectively nullified privacy as an independent right under the then-prevailing Indian law system.

Similarly, the Court dealt with police surveillance in *Kharak Singh v. State of U.P.* (1963), that is, the legitimacy of police late-night visits to the residences of suspected criminals. The Court held that such surveillance breached the right of personal liberty afforded by Article 21 of the Constitution since it constituted an incursion into one's private domain. But, once more similar to *M.P. Sharma*, the majority judgment did not recognize a general right to privacy. Instead, it focused on the specific nature of the police actions being unconstitutional.¹³

Justice Subba Rao's dissent in *Kharak Singh* was noteworthy, notwithstanding the majority's position. Since personal liberty cannot be completely safeguarded without the protection of privacy, Justice Subba Rao argued that the right of privacy could be included within the right to personal liberty under Article 21. His dissenting judgment formed the premise of subsequent legal arguments that would broaden India's definition of privacy rights.¹⁴ Justice Subba Rao's view remained influential and contributed to the gradual reinterpretation of constitutional rights, especially as privacy became a central

¹² *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

¹³ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

¹⁴ (Subba Rao, J., dissenting).

issue in later cases.

As privacy became a major concern in subsequent instances, Justice Subba Rao's opinion continued to have sway and helped to gradually reinterpret constitutional rights. Future judicial views on privacy were significantly shaped by Justice Subba Rao's dissent. Later seminal rulings, such as *K.S. Puttaswamy v. Union of India* (2017), which created the right to privacy as a basic right under the Indian Constitution, finally embraced his approach that privacy is a component of personal liberty. Although it first seemed like a minority opinion, the disagreement eventually contributed to the rethinking of India's constitutional provisions, making privacy a crucial component of the country's legal and human rights system.

3.1 *R. Rajagopal v. State of Tamil Nadu* (1994)

In *R. Rajagopal v. State of Tamil Nadu* (1994), the Supreme Court of India provisionally acknowledged the presence of a right to privacy, though one of very limited scope.¹⁵ The lawsuit started when a prisoner's autobiography was published, revealing private facts about his life, including his involvement in illegal activities. Even though privacy is a significant right, the Court held that it can be limited where its limitation advance the public interest, for instance, where public interest trumps the right to privacy of an individual. The decision highlighted that when there is a strong state need, including in cases involving public safety, national security, or other important state interests, privacy may be restricted.

Instead of laying forth a thorough definition or basis for the right of privacy, the Court suggested that its parameters be gradually established by subsequent case law. Because the Court allowed for interpretation and improvement in response to shifting cultural and legal demands, this careful approach allowed the right to privacy to evolve gradually. By adopting this strategy, the Court recognised the value of privacy while also acknowledging that its extent needed to be balanced against other rights and against the interests of the state.

3.2 *People's Union for Civil Liberties (PUCL) v. Union of India* (1997)

This case laid out procedural checks on surveillance under the Telegraph Act, including mandatory recording of reasons and review mechanisms.¹⁶ It was a major milestone

¹⁵ *Gobind v. State of M.P.*, (1975) 2 SCC 148.

¹⁶ *PUCL*, AIR 1997 SC 568.

towards the recognition of surveillance due process and communication privacy.

3.3 *Selvi v. State of Karnataka (2010)*

The Indian Supreme Court examined constitutional validity of forced narco-analysis, polygraph (lie detector) tests and brain mapping in *Selvi v. State of Karnataka (2010)*. These tactics, which are frequently employed in criminal investigations, entail giving medications or using other means to make the person do something against their will, such as divulge information or disclose facts. According to the Court, these actions are against the safeguards provided by Articles 20(3) and 21 of the Indian Constitution.¹⁷

It is not possible to compel anyone to incriminate themselves since under Article 20(3) which protects against self-incrimination. The Court underlined that this fundamental guarantee is violated by these tactics, which entail forcing people to provide information. The state is essentially pressuring people to give self-incriminating evidence by making them go through such processes, which is against Article 20(3).

3.4 *Neera Mathur v. LIC of India*

The Indian Supreme Court addressed the case of obtaining information about individual reproductive health from women workers within the work premises in the case *Government of NCT of Delhi v. Veena Sethi* in 2010. As part of their job requirements, female workers were expected to provide information about their reproductive health, including whether they were pregnant. This practice was at the heart of the dispute. The Court held that such an approach violated the right of informational privacy and denounced it as discriminatory and intrusive. The need that female employees divulge confidential reproductive health information was the subject of this lawsuit. The Court upheld informational privacy in job circumstances and denounced the practice as intrusive and discriminatory.¹⁸

3.5 *K.S. Puttaswamy (Retd.) v. Union of India (2017)*

In *K.S. Puttaswamy (Retd.) v. Union of India (2017)*, a monumental and landmark judgment, a nine-judge bench of the Indian Supreme Court by a ruling held unanimously that privacy is an integral part of the right to life and personal liberty under the Indian Constitution.¹⁹ This was significant as it overruled earlier judgments of courts which had

¹⁷ *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

¹⁸ *Neera Mathur v. LIC of India*, AIR 1992 SC 392.

¹⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

denied privacy a constitutional right and recognized it to be a component of the right to life and personal liberty of Article 21.

The Puttaswamy judgment was a marked departure from the earlier judgments, wherein privacy was not considered to be a fundamental right, i.e., *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of U.P.* (1963). In Puttaswamy, the Supreme Court unequivocally put human dignity and autonomy at the forefront of constitutional protection by reiterating privacy as a fundamental right.

3.6 Post-Puttaswamy Developments

Privacy was invoked in decriminalizing homosexuality in *Navtej Singh Johar v. Union of India*.²⁰ Homosexual acts, which had been criminalized under Section 377 of the Indian Penal Code, were declared unconstitutional and therefore struck down by the Supreme Court of India in *Navtej Singh Johar v. Union of India*, decriminalizing consenting same-sex relationships. Recognising that sexual orientation and interpersonal relationships are aspects of human liberty and dignity, the Court grounded its ruling in the basic right to privacy. An important milestone towards LGBTQ+ rights in India was the verdict, which upheld people's freedom to choose their sexual orientation without government intervention.

The Section 497 of the Indian Penal Code regarding adultery was overruled by the Supreme Court in *Joseph Shine v. Union of India*, which made extramarital encounters illegal but only applied to males; women were not included. The Court ruled that this legislation is discriminatory and contravening the right to equality (Article 14) as well as the right to privacy (Article 21).²¹

It continues to inform debates around Aadhaar and the Data Protection Act, forming the backbone of India's digital rights jurisprudence.

²⁰ *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.

²¹ *Joseph Shine v. Union of India*, (2019) 3 SCC 39.

4. INTERNATIONAL PERSPECTIVE OF RIGHT TO PRIVACY

4.1 Universal Declaration of Human Rights (UDHR)

The first international expression of inalienable human rights, the Universal Declaration of Human Rights (1948), set the theoretical foundation for privacy law throughout the world. "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence," Article 12 states. The UDHR has been an inspiration for many national constitutions and accords, although not being legally obligatory. Its privacy clause is essential for highlighting how essential privacy is to human autonomy and dignity. This clause has been used as the foundation for draughting or interpreting privacy rights in national frameworks around the globe. The UDHR influenced the Constitution's draughting for India and was a reliable source for constitutional interpretation, particularly in rulings such as Puttaswamy.

4.2 International Covenant on Civil and Political Rights (ICCPR)

Enacted in 1966 and ratified by India in 1979, the International Covenant on Civil and Political Rights (ICCPR) is a binding treaty that obliges the member states to defend civil and political rights. Like Article 12 of the UDHR, Article 17 of the ICCPR also explicitly states that "no one shall be subjected to arbitrary or unlawful interference with his privacy."²² The right to legal protection against such interferences is likewise covered by the clause. The Human Rights Committee, responsible for the implementation of the ICCPR, has emphasized that data collection, monitoring, and searches by a state must be mandatory under the law and must be necessary and appropriate. Indian courts, in construing Article 21, have oftentimes referred to the provisions of the ICCPR, particularly when they are discussing surveillance and individuals' rights to their personal information.

4.3 European Convention on Human Rights (ECHR)

Arguably the most significant of the human rights conventions, the ECHR was signed in 1950 and has robust enforcement through the European Court of Human Rights. "Respect for private and family life, home, and correspondence" is ensured in Article 8."²³ By creating rights against arbitrary intrusions by public agencies, illegal data retention, and

²² International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

²³ European Convention on Human Rights, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

monitoring, the ECHR has made substantial contributions to the doctrine on privacy. Famous rulings like *Von Hannover v. Germany* shielded prominent persons' privacy from media intrusion, while *Klass v. Germany* maintained monitoring only when subject to judicial supervision.²⁴ These choices have become international norms for reconciling the rights of individuals and the public interest. In decisions such as *Rajagopal and Puttaswamy*, the influence of ECHR case law can be seen.

4.4 American Convention on Human Rights (ACHR)

The Pact of San José Costa Rica (1969), also known as the ACHR, contains privacy protections in Article 11. It protects individuals from “arbitrary or abusive interference with his private life, his family, his home, or his correspondence.”²⁵ These rights are assured by the Inter-American Court of Human Rights, particularly where there is state monitoring or a breach of personal information. The ACHR's privacy framework demonstrates a thorough regional commitment to civil rights, notwithstanding India's non-participation in this convention. This has inspired similar developments in other regions of the world. Its jurisprudence offers comparative perspectives that are pertinent to the changing legal landscape in India.

4.5 Convention on the Rights of the Child (CRC)

Article 16 of the CRC ensures children against arbitrary or unlawful interference with privacy, the home, or the family.²⁶ Concerns have been expressed about topics like digital consent, targeted advertising, and online monitoring as kids use the internet more and more. The CRC's focus on protecting data that is sensitive to children is becoming more and more pertinent. This has sparked conversations about digital platforms, kid data protection in educational institutions, and age-appropriate material regulation in India. The CRC sets high standards for domestic legislation by requiring that all data processing and surveillance be done in the best interests of children.

4.6 United Kingdom

The ECHR has been incorporated within domestic laws through the Human Rights Act of 1998 in the UK, which gives British courts the authority to enforce Article 8's privacy rights. *Campbell v. MGN Ltd.* is a landmark case in which the House of Lords upheld the

²⁴ *Klass and Others v. Germany*, App. No. 5029/71, 2 Eur. H.R. Rep. 214 (1978); *Von Hannover v. Germany*, App. No. 59320/00, 40 Eur. H.R. Rep. 1 (2004).

²⁵ American Convention on Human Rights, art. 11, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123.

²⁶ Convention on the Rights of the Child, art. 16, Nov. 20, 1989, 1577 U.N.T.S. 3.

right of an eminent personality to privacy after unauthorized publication of her private medical information.²⁷ A move towards a stronger protection of individual liberty was reflected in this judgement, which established the tort of "misuse of private information." Statutes such as the Data Protection Act, which has been revised in accordance with GDPR, have also developed UK privacy law. India should take inspiration from these achievements, which demonstrate how common law ideas can be integrated with statutory and international commitments.

4.7 United States

The U.S. Supreme Court has construed privacy in a series of amendments, including the First, Fourth, and Fourteenth, despite the fact that the U.S. Constitution does not specifically mention privacy. Citing a "zone of privacy," the Court struck laws prohibiting the use of contraceptives inside marriage in *Griswold v. Connecticut*.²⁷ Later, in *Roe v. Wade*²⁸, the Court recognized privacy in reproductive choices, and in *Katz v. United States*²⁹, it articulated the principle of a "reasonable expectation of privacy." Global legal debate has been greatly influenced by U.S. privacy jurisprudence. In contrast to more centralised models like the GDPR, privacy regulation in the United States is still decentralised and managed by sector-specific regulations like the Privacy Act (for federal agencies) and HIPAA (for health data).

4.8 Australia

Australia does not have a constitutionally guaranteed right to privacy, but statutory protections are available under the Privacy Act 1988 (Cth).³⁰ The Act creates the Australian Information Commissioner as the monitoring body and controls the processing of personal data by government organisations and departments. Although more general jurisprudence is still cautious, courts have nevertheless acknowledged a limited tort of privacy under some circumstances. Indian data protection regimes can benefit from the lessons learnt from Australia's legal approach in the areas of administrative enforcement, consent models, and regulatory independence.

5. CONCLUSION

One of the landmark developments in constitutional law was achieved when the Indian

²⁷ *Griswold v. Connecticut*, 381 U.S. 479 (1965).

²⁸ *Roe v. Wade*, 410 U.S. 113 (1973).

²⁹ *Katz v. United States*, 389 U.S. 347 (1967).

³⁰ Privacy Act 1988 (Cth) (Austl.).

Constitution itself recognized the right to privacy as a fundamental right. It is the growing worldwide view that privacy is a necessary component of autonomy, liberty, and dignity. Indian courts were initially hesitant to recognize privacy as a fundamental right, with limited recognition in cases such as *M.P. Sharma and Kharak Singh*.³¹ But that line of thought has been transformed by decades of judicial evolution with the *Puttaswamy* judgment that treated privacy as an inalienable constituent of Article 21 of right to life and liberty.

By offering a doctrinal framework that incorporates a three-pronged examination of legality, need, and proportionality, the *Puttaswamy* ruling did more than just declare something; it revolutionised constitutional law. It strengthened privacy as the cornerstone of individual freedom by influencing later decisions in crucial areas like the decriminalisation of same-sex partnerships (*Navtej Singh Johar*) and adultery (*Joseph Shine*).³² India's rights-based constitutional approach is founded on the understanding that privacy safeguards a variety of interests, such as physical integrity, informational autonomy, and decisional freedom. Even with this strong legal basis, there are still issues with the practical application of privacy rights. Despite government programs like Aadhaar and the increasing digitisation of services, India does not have a strong legal framework for the protection of personal data. There is no independent control of intelligence or law enforcement organisations, and the nation's surveillance infrastructure functions with little openness. Furthermore, people frequently don't know they have the right to privacy, particularly in rural and underprivileged areas. Rapid technological advancement, state capacity constraints, and a regulatory disconnect between executive activities and court protections all contribute to these problems.

The potential of over-collection, profiling, and monitoring has increased as India's digital infrastructure continues to rise. Because there is frequently little oversight of the private sector, especially big digital companies, user data may be used without meaningful permission or responsibility. The privacy rights discourse is severely lacking as a result of the absence of public discussion surrounding algorithmic governance, predictive policing, and face recognition technology. It is urgently needed to bridge the gap between constitutional ideals and effective enforcement mechanisms.

³¹ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300; *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

³² *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1; *Joseph Shine v. Union of India*, (2019) 3 SCC 39

REFERENCES**BOOKS**

1. Pandey J. N., Constitutional Law of India, (Central Law Agency, Allahabad, 40th ed. 2003).
2. Basu P, Law Relating to Protection of Human Rights under the Indian Constitution and Allied Laws, (Modern Law Publications New Delhi 2007).
3. Chandra U, Human Rights (Allahabad Law Agency Publications, Allahabad, 5th ed. 2004).
4. Jain M. P., Indian Constitutional Law, (Wadhwa and Company, Nagpur, 5th ed. Reprint, 2005).
5. Sharma, S, Privacy Law: A Comparative Study, (Atlantic Publishers and Distributors, New Delhi, 1994).

JOURNAL ARTICLES

1. Deshta S —Right to Privacy: An Extension of Personal Liberty|| (2005) M.D.U. Law Journal, Vol. X (1) PL7.
2. Adithan V —Right to Privacy under Article 21|| (2003) Madras Law Journal Vol. I PL 11.
3. Ahmad M —Muslim Law and Reforms: Protection of Privacy in Islam|| (2000) Civil and Military Law Journal Vol. 36 PL 73.
4. Awasthi S —Privacy Laws in India: Big Brother is Watching You|| (2002) Company Law Journal Vol. 3 PL 49.
5. Bajwa D —Right to Privacy – its Origin & Ramifications|| (1990) Civil & Military Law Journal Vol. 26 PL 66.
6. Gupta S —Right to Privacy is an Aspect of Human Dignity”, Journal of Legal Studies|| (1985) Vol. 17, PL 31.
7. Bhandari M —Right to Privacy Versus Freedom of Press: A Comparative Conspectus of Legal Position in U.S.A., U.K. and India|| (1991) The Indian

Journal of Legal Studies, Vol. XI PL 47.

8. Bharuka D —Piercing the Privacy Veil: A renewed threatl (2003) Supreme Court Cases Vol.1 PL 77.

STATUTES

1. The Code of Criminal Procedure, 1973
2. The Constitution of India, 1950
3. The Indian Penal Code, 1860
4. The Indian Easement Act, 1882
5. The Information Technology Act, 2000
6. The Reserve Bank of India Act, 1934

CONVENTION S

1. European Convention on Human Rights, 1950
2. American Convention on Human Rights ,1967
3. American Convention on Human Rights, 1969
4. Convention on the Rights of Child, 1989
5. International Covenant on Civil and Political Rights, 1966

ONLINE SOURCES

1. SCC Online
2. Manupatra