*Page: 1864-1891* *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

# LawFoyer International Journal of Doctrinal Legal Research

**[ISSN: 2583-7753]**

**Volume 3 | Issue 4**

**2025**

*DOI: https://doi.org/10.70183/lijdlr.2025.v03.203*

# RIGHT TO PRIVACY, A FUNDAMENTAL RIGHT: A CASE STUDY ON JUSTICE K. S. PUTTASWAMY (RETD.) & ANR. V. UNION OF INDIA & ORS., 2017

**Fannana Mazumder**[1]

## I. ABSTRACT

*Right to privacy is a complicated concept that has evolved over time and was affected by various factors. It is a multifaceted aspect which differs from person to person that seems to be easy but difficult to define. Right to privacy, in layman's words, can be defined as the impalpable as well as physical right of any person to live freely from others' interference or intrusion. The idea of privacy is a vague one having an intricate value. Right to privacy can also be defined as one's freedom of choice. The Right to Privacy is a fundamental aspect of human liberty and dignity. In India, right to privacy was recognized as a fundamental right under Article 21 of the Indian Constitution by the Supreme Court in the case of Justice K. S. Puttaswamy (Retd.) & anr. v. Union of India & ors., 2017. This case was a historic judgement that unanimously recognized Right to Privacy as a fundamental right. The historic judgement was delivered by a nine-judge bench of the Supreme Court of India in the year 2017. The case originally arose when Justice K. S. Puttaswamy, a retired judge of the Karnataka High Court via writ petition moved to Supreme Court challenging the constitutionality of the Aadhar Scheme on the grounds that it violated the citizens' right to privacy. The primary issue in this case was that whether the right to privacy was an intrinsic part of right to life and personal liberty guaranteed under Article 21 of the Indian Constitution and a part of the freedoms guaranteed under Part III of the Constitution. The Supreme Court of India in its nine-judge bench unanimously delivered judgement, recognized right to privacy as a fundamental right and an intrinsic part of right to life and personal liberty guaranteed under Article 21 of the Constitution of India. It was also held that right to privacy is also a part of the freedoms guaranteed under Part III of the Constitution. The Court overruled the earlier judgments in the cases of M. P. Sharma v. Satish Chandra, 1954 and Kharak Singh v. State of Uttar Pradesh, 1964, where it was held, that right*

[1] Student, LLM, 1st semester, IILM University, Greater Noida (India). Email: fannana.mazumder.gnllm2026@iilm.edu

*to privacy was not a fundamental right. This case emphasized that any infringement on the right to privacy must satisfy the conditions of legality, necessity and proportionality. The judgement also emphasized that privacy extends to all spheres of life including individual freedoms, data protection and sexual orientation. This historic judgement laid the groundwork in the case of Navtej Singh Johar v. Union of India, 2018 for decriminalization of homosexuality. This case was a game changer in the context of individual freedom in India marking the beginning of a historic legal battle.*

## II. KEYWORDS

Right to Privacy, Fundamental right, Article 21, Right to life and personal liberty, Indian Constitution, Supreme Court of India, Aadhar.

## III. INTRODUCTION

Though deeply ingrained in human civilization since time immemorial, the concept of privacy has recently gained explicit legal and constitutional recognition in India. In a democratic society like that of India which is governed by the principle of 'rule of law,' the constitution is the primary legislation that governs individual autonomy, dignity and liberty. Right to privacy as a fundamental right was recognized in the historic judgement of the K. S. Puttaswamy (retd.) & anr. v. Union of India & ors.[2] given by the Supreme Court of India representing one of the most transformative moments in the constitutional history of India. The decision not only laid a legal and constitutional foundation for protecting personal liberty in today's digital era but also opened a new front balancing the relationship between individual and the State.

The Indian Constitution does not explicitly enumerate "privacy" as a fundamental right but is interpreted under Article 21 of the constitution that guarantees individual the right to life and personal liberty. Earlier, the decisions laid down in the cases of M. P. Sharma v. Satish Chandra[3] and Kharak Singh v. State of Uttar Pradesh[4] denied the existence of privacy as a constitutional right, thus before the Puttaswamy judgement,

[2] Justice K. S. Puttaswamy (retd.) v. Union of India, AIR 2018 SC (SUPP) 1841
[3] M. P. Sharma & ors. v. Satish Chandra, 1954 SCR 1077
[4] Kharak Singh v. State of Uttar Pradesh & ors., AIR 1964 SCR (1) 332

the Indian Judiciary system did not recognize privacy also to be read with Part III of the Constitution.

The evolution of technology raised a serious question on the protection of privacy in India. The Aadhar scheme which required the biometric and demographic data of individuals for the verification of identity making the judicial authorities bound to reconsider the constitutional status of privacy. Thus, a retired judge of the Karnataka High Court named K. S. Puttaswamy moved to the Supreme Court of India challenging the constitutional validity of the Aadhar scheme by filing a PIL. The collection of personal data without adequately safeguarding the privacy and dignity of an individual was contended by the petitioner. The issue was therefore put forward a nine- judge constitutional bench and the unanimous judgment having far- reaching implications. It also is a guiding principle for balancing individual rights to privacy and the State's legitimate goal to ensure national security and public order. The Court introduced the 'proportionality test' that provides a systematic and structured method to draw a conclusion that whether in a democratic society it is justified for State to interfere with privacy.

The Supreme Court in its unanimous verdict held the Right to Privacy as a fundamental right under the Article 21 of the Indian Constitution and integral part of the Part III of the Constitution overruling the judgment passed in the cases of M. P. Sharma and Kharak Singh cases. The Court observed that privacy is natural and inalienable right that human beings inherit by virtue of their existence and not a gift from the State.

The historic landmark judgement harmonized Indian constitution with global trends symbolizing India's evolving judiciary to protecting individual rights in increasingly technological world. The judgements emphasis on individual dignity and liberty influenced future rulings such as the Navtej Singh Johar case dealing with the LGBTQ section of the society.

The recognition of the right to privacy as a fundamental right thus is a reaffirmation of the Constitution's vision of a free and dignified existence for humans and not just a simple judicial creativity. The Puttaswamy case is a constitutional milestone erasing

the gap between individual liberty and collective governance resulting in India's entry into a new era.

### A. Research Objectives

1. To examine the constitutional evolution of the right to privacy in India with special reference to the judgment in *Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, 2017.
2. To analyse the doctrinal shift from earlier judicial pronouncements such as *M. P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh* to the recognition of privacy as a fundamental right.
3. To study the dimensions of privacy including physical, informational and decisional privacy as recognised by the Supreme Court.
4. To evaluate the effectiveness of the proportionality test laid down in the Puttaswamy case in balancing individual liberty and State interests.

### B. Research Questions

1. How did the Supreme Court of India evolve the right to privacy into a fundamental right under Article 21 of the Constitution in the Puttaswamy case?
2. In what manner did the Puttaswamy judgment depart from the earlier rulings in *M. P. Sharma* and *Kharak Singh*?
3. What are the various dimensions of privacy recognised by the Supreme Court in the Puttaswamy case?
4. How effective is the proportionality test in ensuring a balance between individual privacy rights and the legitimate interests of the State such as national security and public order?

### C. Research Hypotheses

1. The judgment in *Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* has fundamentally transformed the constitutional status of privacy in India by recognising it as an intrinsic part of Article 21.

2. The earlier judicial approach denying privacy as a fundamental right was inconsistent with the evolving concept of human dignity and personal liberty.
3. The proportionality test laid down in the Puttaswamy case provides a constitutionally sound framework for assessing State interference with the right to privacy.
4. Despite constitutional recognition, the absence of a robust legislative framework limits the effective enforcement of the right to privacy in India.

### D. Research Methodology

The present study adopts a doctrinal and analytical research methodology**.** The research is primarily based on secondary sources such as constitutional provisions, landmark judicial decisions of the Supreme Court of India, international conventions, scholarly articles, books and authoritative online legal databases.

The study critically analyses the judicial reasoning in the Puttaswamy case along with earlier precedents including M. P. Sharma v. Satish Chandra, Kharak Singh v. State of Uttar Pradesh, Govind v. State of Madhya Pradesh and PUCL v. Union of India. A comparative approach is also employed to examine international standards on privacy under instruments such as the UDHR and ICCPR. The method of content analysis is used to evaluate judicial trends, doctrinal developments and the practical implications of recognising privacy as a fundamental right.

### E. Literature Review

Several scholars have analysed the evolution of the right to privacy both in international and Indian contexts. Warren and Brandeis in their seminal article *"The Right to Privacy"* conceptualised privacy as the "right to be left alone", laying the foundation for modern privacy jurisprudence. Alan Westin further expanded the concept by defining privacy as an individual's right to control the flow of personal information.

In India, judicial commentaries on *Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* have recognised the judgment as a watershed moment in constitutional

law. Scholars have highlighted how the decision harmonised Indian constitutional principles with international human rights norms under the UDHR and ICCPR. Articles published in legal platforms such as Supreme Court Observer and LawOctopus have emphasised the doctrinal shift from the restrictive interpretations in *M. P. Sharma* and *Kharak Singh* to a dignity-based understanding of privacy.

However, existing literature also points out the implementation gap, especially in the context of surveillance, data protection and emerging technologies such as artificial intelligence and deepfakes. These scholarly works collectively indicate that while constitutional recognition has been achieved, effective legislative and institutional mechanisms are still evolving.

**F. Statement of problem**

The development of Right to Privacy as a fundamental right in India is a convoluted concept. Before the landmark judgement of the Puttaswamy case Indian judicial system lacked a clear recognition of privacy as a constitutionally protected right.

The growing dependency of humans on technology posed serious threats to personal autonomy, data protection and informational privacy of individuals. Individuals were exposed to easy misuse of personal data by both State and anonymous authorities or individuals in the absence of a strict and robust legal framework protecting privacy.

Although the Puttaswamy case recognized privacy as a fundamental right, many questions remain unanswered, these are-

1. How the Supreme Court laid principles be effectively operational within India's existing legal and policy framework?
2. How can State balance the right to privacy with their aim to achieve national security and public order?
3. What are the limitations of the current framework in upholding privacy?

The main problem thus lies in assessing the practical implication of constitutional recognition of the right to privacy and upto what extent the Indian legal and institutional mechanisms are equipped to uphold this right in the present technologically advancing society.

### G. Need, relevance and importance of study

The implications of the Puttaswamy judgement extend beyond its declaratory value, raising essential questions regarding the implementation, scope and limitation of the governance in regard to privacy.

The increasing intersection between law, technology and individual freedom arises the need to study of the right to privacy as a fundamental right. This research aims to understand the ability of India's legal system to ensure that technological growth does not pose a threat to human dignity, autonomy and privacy.

The relevance of this study can be pointed out by the following-

1. The growing digitalization and the introduction of large- scale data collection schemes.
2. The lack of specific legislation dealing with data protection.
3. The increasing recognition of privacy as a universal human right aligning with international conventions like the UDHR and ICCPR to which India is a signatory to.
4. The necessity to evaluate how Indian constitutional framework aligns with global standards on privacy and human rights.

By critically analysing the Puttaswamy case, this research will explore legal foundations, doctrinal evolution and practical implications of right to privacy as a fundamental right. The importance of the study lies as it helps in identifying the loopholes in the existing legal system and propose reforms to strengthen privacy protection in the era of expeditious technological and social change.

## IV. RIGHT TO PRIVACY

The Right to Privacy is one of the most important concepts of human liberty that is rooted in the inherent dignity and autonomy of every individual. The term privacy refers to letting an individual live freely from any kind of intrusion, interference or surveillance by the State, other individuals or society.

Privacy means 'the state of being alone and not watched or disturbed by other people' or 'the state of being free from the attention of the public.'[5]

Legally, privacy is not just the absence of intrusion, but the assertion of identity, personal space and decision-making liberty that forms the basis of democratic freedom.

Privacy is a multi-faced concept. Thus, right to privacy protects physical integrity and psychological autonomy of individuals ensuring complete exercising on their freedoms guaranteed under the Indian Constitution. It is connected to the Article 21 of the Constitution of India.

The advent of technologies and artificial intelligence has emerged to be great threat to the privacy of an individual. In today's world where individuals are connected at a global level enabling an exposure to one's personal information online from biometrics, location, to social media activities and financial data. This led to new challenges in protecting informational privacy of individuals as it can be easily misused unconsented.

The Puttaswamy judgement while recognizing privacy as a fundamental right also recognized the need for comprehensive legislation for data protection. Right to privacy though is fundamental but is not absolute. The right to privacy must be balanced against other legitimate interests of the State like national security and maintaining public order. The Supreme Court of India came up with the proportionality test in the Puttaswamy case ensuring that no restriction disproportionately violates individual freedom.

The recognition of right to privacy has far- reaching implications for Indian legal system beyond just its constitutional significance. Thus, the right to privacy emerges as an important aspect for constitutional democracy. The Puttaswamy judgement transformed privacy from an intangible claim to a tangible constitutional right.

[5] Definition from Oxford Languages

## V. BACKGROUND OF PRIVACY AND THE JUSTICE K. S. PUTTASWAMY CASE

Privacy is an ancient concept that has evolved over time. While it was not laid down in any comprehensive legal framework specifically, privacy is something that is inherent to humans by virtue of their birth.

In western philosophy, John Locke's 'Natural Justice Theory' and John Stuart Mill's idea of 'individual liberty' laid the foundational framework for privacy. People started going to courts to open personal letters since the 14th century.

After opposing the first US census in the year 1970, concerns on privacy began that resulted in private family affairs could no longer be disclosed to neighbours.

By the end of 19th century, in the year 1873, the first complaint was recorded about intrusive interview techniques. Later, the invention of portable cameras made it easier for journals to click instant photographs of private moments and publicize it. To counter this, in the year 1890, Samuel D. Warren and Louis Brandeis wrote 'The Right to Privacy' which was punished as an article in the Harvard Law Review, arguing that modern having rapid technological advancements especially the invention of cameras and expanding press posed serious threats on personal autonomy. They articulated privacy as 'the right to be left alone.'

After World War II, privacy as a fundamental human right emerged as international recognition. This resulted in the Universal Declaration of Human Rights (UDHR) in Article 12 and the International Covenant on Civil and Political Rights in its Article 17 recognized privacy as a right of every individual to be protected from any kind of arbitrary interference.

By the mid-20th century, data collection tools began to develop, raising serious concerns on privacy. Alan Westin in his book "Privacy and Freedom" defined privacy as the right of an individual to decide 'when, how and to what extent' personal information can be shared. This book became one of the most important works on privacy even in the modern era.

In the present 21st century, the rapid growth of internet that even connects cross-borders, though having positive impact, emerged to be a serious threat to privacy. Many countries like the European Union, United States, China, etc. came up with regulations that governed privacy rights especially in the era of synthetic media and AI.

## VI. PRIVACY IN INDIA

Though India is a signatory of the international conventions, Indian Constitution did not recognize privacy as a fundamental right explicitly. The framers of the Constitution did not include the term 'privacy' while guaranteeing rights under Part III of the Constitution. As a result of this, privacy in India was left to be recognized by constitutional evolution and judicial interpretation.

Privacy approach of the Indian Judiciary was inconsistent. Two early cases notably shaped like this course-

### A. M. P. Sharma & ors. v. Satish Chandra[6]

In this case, the petitioners moved to the Supreme Court via Article 32 of the Indian Constitution challenging the validity of the warrants after a company went into liquidation and the investigation after alleged misappropriation of funds, producing false balance sheets, etc. The petitioner argued that the investigation violated their rights enshrined under Article 19(1)(f) and Article 20(3) of the constitution.

The eight-judge bench of the Supreme Court ruled that the framers of the constitution did not recognize privacy as a fundamental right and thus right to privacy is not a fundamental right, upholding the practice of search and seizure.

### B. Kharak Singh v. State of Uttar Pradesh[7]

In this case, Kharak Singh filed a writ petition challenging the surveillance tactics of the police under U. P. Police Regulations with the Supreme Court. The petitioner was subject to intrusive and intense surveillance throughout the clock when he was being

[6] M. P. Sharma & ors. v. Satish Chandra, 1954 SCR 1077
[7] Kharak Singh v. State of Uttar Pradesh & ors., AIR 1964 SCR (1) 332

tried for being a part of an armed robbery. This particularly raised the question whether right to privacy and personal is guaranteed under Part III of the Constitution.

The Court ruled that privacy is not guaranteed as a constitutional right though it upheld personal liberty.

1. **Expansion of privacy in India-**

In the case of Govind v. State of Madhya Pradesh,[8] similar to Kharak Singh, Govind challenged the validity of the Madhya Pradesh Police Regulations. He claimed to be beaten by police officers many times on their regular visit to the prison. Govind challenged Regulations 855 and 856 saying that they were not in accordance with the right to privacy.

The Supreme Court of India borrowing from the American Jurisprudence introduced the 'compelling state interest test.' The Court recognized privacy as a fundamental right but subjected to reasonable restrictions for the states interest at large.

2. **Recognition of informational privacy in India-**

In the case of PUCL v. Union of India,[9] the petitioner which was a voluntary organization filed a PIL challenging Section 5(2) of the Indian Telegraph Act, 1885 claiming that it violated individuals right to privacy after Central Bureau of Investigation published a report on 'Tapping of Politicians Phones.'

The Court noted that Indian Constitution did not explicitly recognize right to privacy, but it was a part of Article 21 and cannot be curtailed until and unless provisions established by law.

In the context of phone tapping, the Court recognized right to privacy as a part of Article 19 (1) (a) guaranteeing freedom of speech and expression.

3. **The landmark judgement on privacy in India-**

Finally in the case of Justice K. S. Puttaswamy (retd.) v. Union of India,[10] a nine- judge constitutional bench unanimously recognized right to privacy as a fundamental right

[8] Govind v. State of Madhya Pradesh, AIR 1975 SC 1378
[9] PUCL v. Union of India, AIR 1997 SC 568
[10] Justice K. S. Puttaswamy (retd.) v. Union of India, AIR 2018 SC (SUPP) 1841

under Article 21of the Constitution of India that guaranteed individuals the right to life and personal liberty.

## VII. ARTICLE 21 OF THE INDIAN CONSTITUTION AND RIGHT TO PRIVACY

Article 21 of the Indian Constitution declares - "Protection of life and personal liberty- No person shall be deprived of his life or personal liberty except according to procedure established by law."[11]

This short provision has been described as the heart of the Indian Constitution. The framers of the constitution saw Article 21 as a safeguard against arbitrary curtailment of liberty by the State. The interpretation of this Article was narrow initially, but as time passed by, the Supreme Court of India transformed this Article into dynamic hub of unenumerated fundamental rights essential to lead a dignified human life.

With the advent of technology, new challenges emerged posing serious threats to privacy. Thus, the right to privacy was recognized as a fundamental right by the Supreme Court in the case of Justice K. S. Puttaswamy (retd.) v. Union of India guaranteed under Article 21and a need for a comprehensive legislation governing data protection was emphasized by the Court.

## VIII. THE JUSTICE K. S. PUTTASWAMY (RETD.) V. UNION OF INDIA CASE

On 24th August 2017, Supreme Court of India affirmed the right to privacy as an integral part of the Part III of the constitution in the landmark case of Justice K. S. Puttaswamy (retd.) v. Union of India creating a constitutional history.

**FACT:**

The Government of India on 29th September 2010 launched the Aadhar Scheme nationally which was a Unique Identification (UID) Program that required the biometrics of an individual. Justice K. S. Puttaswamy, a retired judge of the Karnataka

[11] INDIAN CONST. art. 21

High Court, moved to the Supreme Court challenging the Aadhar scheme, asserting that the collection of biometrics is a violation of the privacy rights of an individual.

**ISSUES RAISED:**

The main issues that were raised before the Supreme Court were-

1. Whether the right to privacy is a fundamental right under the Indian Constitution despite not being explicitly provided?
2. Whether the Aadhar scheme violated right to privacy?

**PETITIONERS' ARGUMENT:**

The petitioner challenged the judgement passed in the cases of M. P. Sharma and Kharak Singh and cited the A. K. Gopalan[12] and Maneka Gandhi[13] cases. He also advocated for a multi- dimensional broad understanding of privacy aligning with the international conventions and natural rights theory. The petitioner proposed that right to privacy was an integral part of Article 21 guaranteeing right to life and personal liberty. Thus, court as a protector of rights has the duty to safeguard this right.

**RESPONDENTS ARGUMENT:**

Respondents citing the judgment passed in the cases of M. P. Sharma and Kharak Singh argued the right to privacy was not explicitly mentioned in the Constitution and reading it with Article 21 would result in judicial overreach. Privacy was regarded as an ambiguous concept in the eyes of the respondents and should be defined through legislative processes.

**JUDGEMENT:**

The Supreme Court held that right to privacy is a fundamental right under Article 21 of the constitution. The court further stated that though privacy is fundamental, it is not absolute and restricted by law in case of legitimate interests of the State.

The judgement stressed on two fronts of privacy-

[12] A. K. Gopalan v. The State of Madras, AIR 1950 SC 27
[13] Maneka Gandhi v. Union of India, AIR 1978 SC 597

1. The right to be left alone without the state's interference in personal matters.
2. The right to autonomous decision- making without undue interference.

The court recognized various dimensions of privacy such as informational privacy, decisional privacy, etc.

The court emphasized the need for a robust legal framework particularly dealing with data protection. The judgement also addressed the marginalized sections of the society such as the LGBTQ community ruling that sexual orientation is a core part of personal liberty thus guaranteed under Article 21.

**A. Dimensions of right to privacy recognized in the Puttaswamy case**

The Supreme Court of India in the Puttaswamy case identified various dimensions of privacy-

1. Physical privacy - Protection of individuals from bodily intrusion and surveillance.
2. Informational privacy - Individuals have the right to protect and control their personal data and digital identity.
3. Decisional privacy - Individuals have complete autonomy in making personal choices.

These dimensions reflect that privacy has far-reaching seclusions.

**B. The Proportionality Test**

The advent of technology has sparked one of the most complex debates and raised questions on- 'how to balance the right to privacy with the right to freedom of speech and expression.' Both the rights are fundamental rights of an individual guaranteed by the Constitution of India.

Though malicious technological use involves creating non- consensual pornography, identity fraud, political misinformation, etc., but on a positive spectrum not all the uses of technology are malicious, some are used to entertain, educate and gain knowledge on various fields like politics, happenings in society, etc. Thus, a complete

ban on the creation of content using technology might result in curtailing the artistic freedom and technological innovation of individuals.

Thus, to create a balance, the historic judgment of the Puttaswamy case gave a proportionality test that must be applied while imposing ban on any content. This test ensures that whether a restriction that is imposed on the fundamental right of the individual by the State is constitutionally valid and justified.

The Court laid down a four- fold proportionality test -

1. **Legality:** Any restriction imposed must have a legal basis and reasoning. There must be a valid law or legal foundation passed by a legislature that authorizes the restriction. The action of the State curtailing fundamental rights must not be arbitrary.
2. **Legitimate aim:** The restrictions imposed must have legitimate aim in accordance with law such as serving the purpose of maintaining national security, prevention of crime, etc. Thus, the restrictions imposed must be necessary for the democratic society.
3. **Rational connection or proportionality:** The action imposed must be necessary to achieve the goal and it should not be excessive in scope. Thus, there must be a rational nexus between the State's action and the intended goal. The extent of interference by State must be such that is proportionate to the necessity of such interference.
4. **Necessity and balance test:** In case a less intrusive restriction is available that serves the same purpose, then, the more intrusive way becomes unconstitutional. The measure taken to curtail the fundamental right must be the least intrusive way to achieve the intended goal. Courts must maintain a balance between individual rights and public interest to make sure that it does not account for disproportionality. These interferences must have procedural guarantees.

**C. Implications of the Puttaswamy judgement**

1. Some parts of the Aadhar Act were upheld subject to privacy safeguards.

2. It laid down the constitutional foundation for data protection laws resulting in the Digital Personal Data Protection Act in the year 2023.
3. It strengthened judicial scrutiny over surveillance regimes, bodily autonomy like sexual orientation and media intrusion.
4. It laid the groundwork of the Navtej Singh Johar v. Union of India, 2018[14] case that decriminalized homosexuality.
5. It harmonized Indian constitutional principles with international human rights norms and international conventions.

**D. Challenges post Puttaswamy judgement**

Though the Puttaswamy judgement transformed the constitutional landscape of India, its effective implementation in legislative, administrative and technological safeguards has proven to be a complex task.

1. **Lack of comprehensive legal framework and enforcement mechanism** - Although the Puttaswamy judgment emphasized the need of a comprehensive data protection legislation, India found it difficult to create privacy regime that meets constitutional and international standards. Though the DPDP Act, 2023 is a major step towards codifying privacy norms, it has a lot of drawbacks –
   - The Act allows the government to exempt any state from compliance on the grounds of 'sovereignty' and 'public order,' suppressing the essence of privacy protection.
   - The Act lacks provisions for strong investigation powers and also lacks full independence leading to weak enforcement.
2. **Surveillance and national security concerns - One** of the most critical challenges posed was in the balancing of individual privacy with states surveillance and security measures. These laws lack transparency, accountability and judicial oversight. India's current surveillance structure

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

does not meet the standards of the proportionality test laid down in the Puttaswamy case.

3. **Technological advancements and emerging threats -** Prior to the Puttaswamy case several technological advancements posed serious privacy threats. The development and rise of artificial intelligence, deepfakes, biometric profiling, etc. created a new challenge that existing laws are incapable of answering. The absence of technological literacy led to lag in enforcement mechanisms.
4. **Conflict between privacy and other fundamental rights -** Despite the Puttaswamy case laying down the proportionality test, balancing privacy with other fundamental rights especially the freedom of speech and expression, right to equality emerged as another challenge. These conflicts are yet to be solved by the legislative and judiciary.
5. **Inadequate awareness and digital literacy -** Public awareness is still lacking in regard to right to privacy. Many citizens are unaware of how their personal data is being collected, synthetic media manipulation, etc. Lack of digital literacy prevents individuals from exercising meaningful control over their data. This makes the constitutional right to privacy an illusion.
6. **Judicial limitations -** The courts can declare rights but cannot always ensure their enforcement. Judicial interpretation alone cannot replace the need for robust legislation and administrative reforms. Thus, weakening post-Puttaswamy accountability mechanisms.

## IX. JUDICIAL CONCERNS ON TECHNOLOGY AND PRIVACY IN INDIA

The landmark judgment given in the Puttaswamy case guarantees right to privacy but the question that now arises is the uniform implementation of it. Indian courts have time and again acknowledged the challenges imposed by technology to privacy.

1. In the case of Anvar P. V. v. P. K. Basheer & ors,[15] the core legal question was the admissibility of electronic evidence such videos and audio CDs. The electronic records were copied from mobile to cameras but no certificate under Section 65B of the Indian Evidence Act, 1872 were produced. The Supreme Court overruled the previous judgment laid down in the case of State (NCT of Delhi) v. Navjot Sandhu[16] and held that Section 65B of the Evidence Act of 1872 was a complete and compulsory provision for the admissibility of electronic evidence. It further held that secondary electronic evidence such as CDs is inadmissible without a valid certificate for the same. The court also distinguished between primary and secondary evidence.
2. In the case of Shreya Singhal v. Union of India,[17] a writ petition was filed under Article 32 of the Constitution challenging the validity of Sections 66A, 69A and 79 of the IT Act, 2000 which were brought into force by the Amendment Act of 2009. The Supreme Court of India struck down Section 66A from IT Act, 2000 that laid down the punishment for sending offensive messages through communication services, etc. stating that it entirely violates Article 19(1)(a) and not saved under Article 19(2). The court further upheld Sections 69A and 79 stating these sections are constitutionally valid.
3. The Delhi High Court in the year 2023, in the case that involved a viral deepfake video of the popular actress Rashmika Mandana recognizing that deepfakes constitute a deep threat to privacy and dignity, directed the government to come up with mechanisms to identify and block such harmful content.[18]

Thus, through these judicial trends we can see the growing tension created by the technological advancements that undermine constitutional guarantees.

[15] Anvar P. V v. P. K. Basheer & ors., AIR 2015 SC 180
[16] State (NCT of Delhi) v. Navjot Sandhu, 2004 Appeal (crl.) 373-375
[17] Shreya Singhal v. Union of India, AIR 2015 SC 1523
[18] The Hindu

## X. INTERNATIONAL CONVENTIONS ON THE RIGHT TO PRIVACY

Globalization, digitalization and rapid technological advancements have increased concerns regarding protection of privacy thus, making it necessary for international norms and conventions to safeguard privacy.

1. **Universal Declaration of Human Rights (UDHR), 1948 -** The Universal Declaration of Human Rights (UDHR) is the first and historic legislation that explicitly recognized the right to privacy proclaimed by the United National General Assembly on 10th December 1948. Right to privacy is recognized under Article 12 of UDHR.

According to Article 12- "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Thus, it establishes privacy as a universal and inalienable human right.

Though UDHR is not legally binding, it has served as philosophical foundations for many conventions, national constitution, etc. The Article 21 of Indian constitution and its recognition of right to privacy was also influenced from the UDHR.

2. **International Covenant on Civil and Political Rights (ICCPR), 1966 -** The ICCPR provides the most authoritative binding international protection of privacy, adopted by the United Nations General Assembly in the year 1966 and was ratified in India in the year 1979. According to Article 17 of the Covenant –
    - No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
    - Everyone has the right to the protection of the law against such interference or attacks."

The principles under Article 17 of the ICCPR resonate strongly with the proportionality test of the Puttaswamy case emphasizing legality, necessity and proportionality for testing states action for interfering in privacy.

3. **Convention on the Rights of Children (CRC), 1989 -** The CRC guarantees privacy rights under Article 16 specifically to minors. CRC was proclaimed in accordance with the principles in the Charter of United Nations.

   According to Article 16 –

   - No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
   - The child has the right to protection of the law against such interference or attacks.

The above provision imposes an obligation on the state to protect and safeguard children's data collection. In this modern era, social media exposure, online tracking, educational data collection, etc. make this protection of utmost importance. As India is a signatory to this convention, thus is obligated to safeguard children's informational privacy.

4. **International Convention on the Protection of All Migrant Workers and Members of their families (ICRMW)** - The ICRMW was adopted by the United Nations General Assembly in the year 1990. It is a comprehensive international treaty aimed at protecting human rights and dignity of migrant workers. Right to privacy is enshrined under Article 14 of the Convention. According to Article 14, "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks." India is not ratified under the ICRMW, but the right to privacy recognized under in the Puttaswamy case aligns with Article 14 of ICRMW, ensuring protection of all individuals including migrants.

# XI. COMPARATIVE PERSPECTIVE- GLOBAL PROTECTION OF PRIVACY

1. **European Union - Transparency, regulation and risk management under the AI Act -** The European Union combines the AI Act dealing with risk-based data protection of AI systems with an existing strong data protection regime, i.e., GDRP. The AI Act classifies AI risk into four categories-
   - Minimal
   - Limited
   - High
   - Unacceptable

   As mentioned in Annexure III of the Act, synthetic media generations involving political and electoral misrepresentation resulting in democratic untrust are categorized as 'high risk.'

   The AI Act requires identifiability measures ensuring transparency for AI generation by clearly labelling them as mentioned under Article 50(3) of the Act. GDRP principles come into force where personal or biometric data are used to build models that produce deepfakes rather than straightaway banning it.

   - Strengths –
     a. It is right- based integrating privacy (GDRP) with specific AI risk control.
     b. Rather than relying only on takedown of content, technical obligations create originator transparency.
     - Drawback - It is complex to comply with small providers and are still being detailed in guidance.
2. **United States - Regulatory patchwork -** The United State lacks a national comprehensive legislation addressing synthetic media especially deepfakes. The Deepfake Accountability Act and the Protect Elections from Deceptive AI Act were introduced after several proposals but have not yet been enacted into law. The Deepfake Accountability Act protects national security by ensuring

transparency in AI generated contents and provides remedies to its victims. The Protect Elections from Deceptive AI Act curtails AI generated deception in political campaigns amending the Federal Election Campaign Act of 1971.

At state level in US there is a growing focus on the generation of deepfakes and regulating it. In the year 2024, 23 states passed legislation governing deepfakes. States have enacted narrow statutes criminalizing deepfakes.

- Virginia's Law criminalizes the generation of deep-fake pornography.
- Callifornia has also established laws that give power to victims to sue in case of non- consensual deepfake pornography.
- Texas has also established laws to criminalize the use of deep-fake technology to defraud others.
- Hawaii enacted laws that ban material content deception during election years, from February to election days.

The United States follows a sectoral approach through privacy torts and specific statutes.

- Strengths –
  a. There are quick legislative responses at state level.
  b. In some states there are civil remedies along with criminal penalties.
- Limitations –
  a. The laws differ from state to state lacking a uniform remedy.
  b. Freedom of expression is risked by invalidating over- board criminal statutes.

3. **China- Deep Synthesis Provisions -** China enacted certain regulations on the Administration of Deep Synthesis of Internet Information Services adopted in the year 2024 that requires providers to label synthetic content, register services and follow real- name obligations. The provisions cover various AI generated content such as images, videos, audios, etc. and also address technological and social challenges imposed by the advent of AI. This regulation opens up a broader front for the Chinese authorities relying on technology to stabilize

society and politics. Thus, this Chinese regulation goes beyond just addressing technological issues but also controls internet to serve national security.

- Strengths -
  a. It ensures clear technical obligations such as labelling synthetic content and strong platform accountability.
  b. It ensures strong administrative enforcement.
- Limitations -
  a. The heavy-handed approach raises questions about freedom of expression and also about surveillance.
  b. The applicability outside China depends on the platform reach.

## XII. LESSONS FOR INDIA WHAT TO ADAPT AND AVOID FROM THE ABOVE FOREIGN LEGISLATIONS

### A. What to adapt:

1. The provenance and labelling from the EU and China model as it enable's AI providers durable watermarks and visible labels over synthetic content.
2. Adapt data- centric controls (GDPR style) that limits unlawful processing of biometric data that is use to train models.
3. Target criminalization by narrow drafting of offences taking caution from US litigation risks.

B. **What to avoid:** The unreasonable bans that risk the legitimate use of technology like journalism, satire, etc. must be avoided.

## XIII. RECOMMENDATIONS TO OVERCOME THE GAPS IN THE EXISTING INDIAN LEGAL FRAMEWORK TO COUNTER THE THREAT POSED BY TECHNOLOGY ON THE RIGHT TO PRIVACY

A. **Enacting a specific regulation that entirely governs modern challenges such as synthetic media generations -** India at present lacks a dedicated statute governing synthetic media related crimes. A specific and comprehensive legislation must be introduced that defines terms like 'deepfake,' 'synthetic media,' manipulated content, etc. The legislation must clearly differentiate between malicious use and legitimate use. The legislation should also provide criminal penalties for synthetic media offences such as non-consensual pornography, electoral misinformation, identity theft, extortion, etc. This legislation must fill the definitional and doctrinal gap that is currently fragmented across various legislations such as IT Act, IPC, etc.

B. **Strengthen the Information Technology Act, 2000 and operationalize the DPDP Act, 2023**

1. The IT Act, 2000 should be amended involving specific provisions for synthetic media, deepfakes and AI generated content and penalize the same.
2. Deepfakes often originate from the misuse of the data that is available online so the DPDP Rules must be amended in such a way that it prohibits the use of facial and voice data for training AI models without explicit consent. The Act should also empower the Data Protection Board of India (DPBI) to issue immediate cease of synthetic data involving personal information. The Act must also allow individuals to demand removal of deep-fakes and seek redressal for damage caused.

C. **Establish a national unit monitoring technological advancements like synthetic media -** A specialized body must be set up by the government under the Ministry of Electronics and IT that will monitor AI generated threats, coordinate with CBI or cyber cell for real- time responses, collaborate with various social media platforms, etc. This unit would be the same as EU's AI Office and China's Cyberspace Administration regulating deep synthesis division.

D. **Mandating provenance and watermarking of AI generated content -** India should follow the EU AI Act and China's Deep Synthesis Regulation to make visible labelling and invisible watermarks of synthetic contents, Penalties for tempering with or removal of watermarks must be imposed. This will ensure traceability guiding for easier investigations.

E. **Strengthen investigative and judicial capacity -** Judicial officers, prosecutors and police must be trained in specialized digital forensics to tackle technological crimes. AI forensics modules must be incorporated in judicial academies and cybercrime training centers. Given the reputational urgency of cases involving deep-fakes, fast track courts must be set up to deal with deepfake cases.

F. **Encourage public awareness -** Public- private partnership for awareness campaigns must be promoted. Media literacy initiatives must be supported to strengthen public discernment against false information.

G. **Promote international cooperation -** Technological crimes are not limited to a specific geography but has cross – border origins and impacts. Thus, India should enter into bilateral or multilateral agreements for sharing of cyber forensics and IP information. India must also participate in global AI governance frameworks such as UN AI Advisory Body, OECDAI Principles, etc. Domestic laws must also be aligned with the MLATs for swift evidence collection. It thus ensures global uniform privacy and authenticity norms.

H. **Integrate proportionality and free expression safeguards -** All the regulatory steps must be in compliance with the proportionality test enshrined in K. S. Puttaswamy case. Such balance sustains constitutional legitimacy while tackling technological harm.

I. **Strengthening accountability in public surveillance -** The increasing deployment of CCTV cameras, facial recognition systems, etc. imposes serious privacy threats. Thus, all surveillance must be subject to judicial oversight and data retention limits. Transparency reports of mandatory surveillance must be published.

## XIV. CONCLUSION

The recognition of Right to Privacy as fundamental right in the Puttaswamy case is a monumental turning point in the development of the Indian Constitution affirming that privacy is not granted by state but is inherent to human existence. The judgment created a harmony between India's domestic laws with international human rights instrument such as the UDHR, ICCPR, etc. India thus, can be aligned within the global constitutional framework upholding privacy as basic to human rights.

The court in earlier judgements of M. P. Sharma and Kharak Singh clearly denied the recognition of privacy as a fundamental right stating that privacy is not explicitly in the Indian Constitution. The Court thus reaffirmed doctrinal dynamism of the Constitution.

The Puttaswamy case has far- reaching implications involving informational privacy, data privacy, decision- making autonomy, physical privacy, etc. It laid down the proportionality test to create a balance between the fundamental right of and individual and the states legitimate interest. This test now serves as the constitutional benchmark for data collection, surveillance, restriction on individual liberty, etc.

Although the Puttaswamy case guaranteed right to privacy, but post- Puttaswamy judgment several challenges posed a threat to its effective implementation. Right to privacy is not an absolute right but is one that must coexist with states' legitimate interest.

The Puttaswamy judgment puts India alongside with constitutional democracies such as European Union, United States, China, etc. recognizing privacy essential to liberty and democracy. The judgement shows India's adherence to international obligations. Thus, Puttaswamy articulated right to privacy represents both legal and moral foundations guiding India to a more just, dignified and right- oriented democracy.

## XV. REFERENCES

### A. Statutes

1. INDIA CONST. art 21

### B. Internet

1. Natalia Moskaleva, A Brief History of Privacy, Criipto, 18 December 2024 https://www.criipto.com/blog/history-of-privacy
2. SCO Team, Right to Privacy: Court in Review, Supreme Court Observer, 4th Jul 2017 https://www.scobserver.in/journal/right-to-privacy-court-in-review/
3. Khushi Malviya, KS Puttaswamy v. Union of India: Landmark case on Right to Privacy, LawOctopus, Oct 28, 2024 https://lawctopus.com/clatalogue/clat-pg/ks-puttaswamy-v-union-of-india-landmark-case-on-right-to-privacy/
4. A.K. Sikri, Justice K.S.Puttaswamy(Retd) vs Union of India on 26 September, 2018, Indian Kanoon https://indiankanoon.org/doc/127517806/
5. Justice K.S. Puttaswamy and Ors. vs. Union of India (UOI) and Ors., Manupatra Academy https://www.manupatracademy.com/legalpost/manu-sc-1044-2017
6. Vajiram Editor, Right to Privacy, Evolution, Significance, Challenges, Nov 1, 2025 https://vajiramandravi.com/upsc-exam/right-to-privacy/
7. Md. Toriqul Islam, A Brief Introduction to the Right to Privacy – An International Legal Perspective, GlobaLex, January/February 2022

https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html

8. Universal Declaration of Human Rights https://www.un.org/en/about-us/universal-declaration-of-human-rights
9. International Covenant on Civil and Political Rights https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
10. Convention on the Rights of the Child https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
11. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-rights-all-migrant-workers
12. Delhi police arrest techie from Andhra Pradesh for Rashmika Mandanna deepfake video, The Hindu, Jan 21, 2024 https://www.thehindu.com/news/cities/Delhi/delhi-police-arrest-techie-from-andhra-pradesh-for-rashmika-mandanna-deepfake-video/article67760419.ece
13. Aditya AK, Proportionality Test for Aadhaar: The Supreme Court's two approaches, Bar and Bench, Sept 26, 2018 https://www.barandbench.com/columns/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches
14. Chaitanya Ramachandran, PUCL V. UNION OF INDIA REVISITED: WHY INDIA'S SURVEILLANCE LAW MUST BE REDESIGNED FOR THE DIGITAL AGE, Manupatra https://docs.manupatra.in/newsline/articles/Upload/E90FA90F-0328-49F2-B03F-B9FBA473964F.pdf