RIGHT TO PRIVACY POST PUTTASWAMY

MS. CHHAVI BHURA

A STUDENT OF UNIVERSITY PF PETROLEUM AND ENERGY STUDIES, SEMESTER V (2021-2026)

INDEX

ABSTRACT

Numerous international treaties recognise the inalienable right to privacy. It is necessary for the safeguarding of human dignity and is a fundamental cornerstone of a democratic nation. It defends both the self and the rights of others.

The relationship between an individual, a group, and an individual that is not vulnerable to interference, unwanted invasion, or infringement of personal liberty is considered private. All modern societies recognise the significance of privacy, not just for humanitarian but also for legal reasons.

When our Constitution was written in the early 1950s, the framers did not think it necessary to add a particular article ensuring the right to privacy.

In a series of decisions, however, the Supreme Court ruled categorically that the Right to Privacy is not a constitutionally protected fundamental right. In 1997, the Apex Court decided People's Union for Civil Liberties (PUCL) v. Union of India, setting the groundwork for the right to privacy in the context of telephonic surveillance (i.e., wiretaps) and constitutional liberties.

This article analysis the Supreme Court's position on the right to privacy in the PUCL Case, which was upheld in the landmark 2017 decision by a nine-judge panel in KS Puttaswamy v. Union of India, in which privacy was deemed a fundamental right.

INTRODUCTION

Privacy is a fundamental right, crucial to autonomy and the protection of human dignity, and serves as the foundation for a great number of other human rights.

This permits us to negotiate who we are and how we wish to engage with the world. Privacy enables us to create limits on who has access to our lives, places, and possessions, as well as our communications and information.

The privacy protection standards enable us to claim our rights in the face of enormous power disparities.

As a result, privacy is a crucial means by which we attempt to safeguard ourselves and society from the arbitrary and unjustifiable use of power, by limiting what can be known about us and done to us, and by shielding us from others who may wish to exert control.

Privacy is crucial to who we are as humans, and we make daily decisions regarding it. It gives us a place to be ourselves without being judged, enables us to think freely without discrimination, and is a crucial factor in providing us power over who knows what about us.

It is no doubt correct that every Government, howsoever democratic, exercises some degree of sub rosa operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day.[1]

WHY DOES PRIVACY MATTER?

In contemporary society, the issue surrounding privacy is a discussion of contemporary liberties.

As we consider how we establish and protect the boundaries around the individual, as well as the individual's ability to have a say in what happens to him or her, we are also attempting to determine:

1. the ethics of modern life;

2. the rules governing the conduct of commerce; and

3. the limitations we place on the power of the state.

[1] PUCL v. Union of India, (1997) 1 SCC 301.

This right has always been interwoven with technology. For instance, our ability to safeguard privacy are higher than ever before, yet surveillance capabilities have never existed before.

We can now uniquely identify individuals amidst massive data sets and streams, as well as make conclusions regarding individuals based on vast data swaths. Companies and governments can now monitor every communication we have, every economic transaction we engage in, and every place we visit. These capabilities may have negative repercussions on individuals, groups, and society as they inhibit activity, discriminate, and exclude. Additionally, they influence how we view the interactions between the individual, markets, society, and the state. In the event that the institutions on which we rely are able to peer into our pasts, observe all of our actions, and predict our future actions, even greater power imbalances will emerge, where individual autonomy vis-à-vis corporations, groups, and governments will effectively disappear, and any deemed aberrant behaviour will be identified, excluded, and even suppressed.

Perhaps the greatest obstacle to privacy is that the right can be violated without the individual's knowledge. You are aware of the interference with other rights, such as when you are arrested, censored, or restricted. With other rights, you are also aware of the transgressor — the official who is detaining you, the censor, offender the police.

We are increasingly not told about the surveillance we are subjected to, nor are we equipped with the means or given the opportunity to question these operations.

As a result of its intrusiveness, lack of accountability, and threat to democratic life, clandestine surveillance, which was formerly employed seldom, is rapidly becoming the norm.

Privacy International envisions a society in which privacy is safeguarded, respected, and realised. Institutions are increasingly exposing people to monitoring and excluding us from decisions over how our lives are disrupted, our information processed, our bodies inspected, and our goods examined. We believe that, in order for individuals to engage in the contemporary world, new laws and technologies must strengthen the right to freely exercise this right, not erode it.

RIGHT TO PRIVACY

The right to privacy is essential to the preservation of human dignity and serves as one of the primary support structures of a democratic state. The right to privacy does not merely refer to the privacy of a person's body; rather, it encompasses an individual's integrity, personal

autonomy, data, speech, consent, objections, movements, and thoughts, as well as their reputation. Each and every contemporary society acknowledges the significance of personal privacy, not just for moral and ethical grounds, but also from a legal one.

The right to privacy is a component of numerous legal systems that restrict government surveillance activities and the corporate sector that endanger the privacy of individuals. In over 150 national constitutions, the right to privacy is recognized.

The right to privacy - by itself - has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case[2].

The Indian Constitution does not guarantee the right to privacy as a fundamental right. However, the Supreme Court, in two recent rulings, has included the right to privacy within the ambit of the fundamental right to 'personal liberty' embodied in Article 21[3].

A recent development in Indian law is the expansion of Article 21's scope, particularly after the Maneka Gandhi v. UOI case[4] (1978). The Supreme Court has repeatedly stated that Article 21 is the bedrock of fundamental rights. Article 21 has demonstrated its complexity. It has been expanded by reinterpreting what constitutes life and liberty in certain circumstances. These words, namely life and liberty, are not universally applicable.

According to Black's Law Dictionary, "right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned".

THE PUTTASWAMY CASE

Prior to 2017, the Apex Court's stance on the right to privacy was somewhat ambiguous. In M.P Sharma v. Union of India[5] (1954), an eight-judge bench of the Supreme Court ruled that the Constitution of India does not protect the right to privacy. In Kharak Singh[6], a constitutional bench of six judges reached the same conclusion (1963).

[2] PUCL v. Union of India, (1997) 1 SCC 301.
[3] [A.G. Noorani], [Right to Privacy], 40 [Economic and Political Weekly] [802], [802] [(2005)].
[4] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[5] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[6] Kharak Singh v. State of U.P., AIR 1963 SC 1295.

However, there were decisions by smaller Supreme Court benches, including R. Rajagopal v. State of Tamil Nadu[7] (1994), it was held that the right to privacy is a constitutionally protected fundamental right, and it was in this context that the PUCL Case was decided.

Justice K S Puttaswamy, a former High Court judge, filed a writ petition with the Supreme Court in 2012 contesting the constitutionality of the UPA government's Aadhaar programme.

On August 11, 2015, a three-judge bench consisting of Justices Chelameswar, Bobde, and C. Nagappan issued an order mandating the examination of the validity of the verdicts in M P Sharma v. Satish Chandra[8], 1954 (Eight Judge Bench) and Kharak Singh v. State of Uttar Pradesh[9], 1964, by a Bench of the appropriate size (Six Judge Bench). Specifically, it instructed the Court to determine whether or not we had a basic right to privacy.

It had argued that the collection and use of personal data of citizens for Aadhaar — now a law under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act[10] of 2016 — improves the lives of millions of poor by granting them direct access to public benefits, subsidies, education, food, health, and shelter, among other fundamental rights. The government asserted that Aadhaar would eradicate corruption in public distribution, money laundering, and terrorism financing.

The Supreme Court's concern over the acquisition and use of data was the possibility of private parties and service providers gaining access to sensitive information.

The government and service providers collect personal information such as mobile phone numbers, bank account information, addresses, date of birth, sexual orientation, health records, property ownership, and taxes without providing protections against unauthorised access.

National programmes such as Aadhaar, RSYB, NATGRID, CCTNS, DNA profiling, reproductive rights of women, privileged communications, and brain mapping entail the collecting and electronic storage of personal data such as fingerprints, iris scans, and physiological samples. The Law Commission has just forwarded a bill regarding DNA profiling of humans. All of this increases the risk of data leaking.

[7] R. Rajagopal v. State of T.N., (1994) 6 SCC 632.
[8] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[9] Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[10] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).

The Supreme Court had frequently inquired whether the government planned to establish a "strong data protection mechanism."

The government informed the Bench that a committee of experts chaired by a former Supreme Court judge, Justice B.N. Srikrishna, was already formed on July 31, 2017 to identify "important data protection concerns" and recommend a draught data protection bill.

This case was initially presented to a five-judge bench led by the then justice Khehar. On July 18, 2017, the dispute was then submitted to a Nine Judge Bench. Chief Justice Khehar and Justices Jasti Chelameshwar, S.A. Bobde, DY Chandrachud, Abdul Nazeer, Nariman, R.K. Agarwal, Abhay Manohar Sapre, and Sanjay Kishan Kaul constituted the Bench. The arguments commenced on July 19, 2017 and ended on August 2, 2017.

Justice D.Y. Chandrachud, while delivering the main judgment, on behalf of the Chief Justice J.S. Khehar, Justice R.K. Agarwal, himself and Justice S. Abdul Nazeer has held that:

"Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian constitution…"[11]

Tracing the evolution of privacy in various cases and writings, the judgment concludes that:

"Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being."[12]

[11] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[12] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

In a landmark ruling handed down on August 24, 2017[13], the Court unanimously acknowledged a basic right to privacy guaranteed by the Constitution, in particular Article 21[14] and broadly Part III. The decisions taken in M.P. Sharma[15] and Kharak Singh[16] were overruled.

INTERNATIONAL IMPORTANCE

As privacy enjoys a robust legal framework internationally, the nine-judge Bench's decision gains international significance, although India has been reticent.

The ruling would have a significant impact on the Aadhaar programme, which collects personal information and biometrics to identify recipients for accessing social benefits and government welfare programmes.

In 2015, a number of petitions contesting Aadhaar as a violation of privacy, informational self-determination, and bodily integrity were filed with the Supreme Court.

The petitioners stated that enrolment in Aadhaar constituted a precursor to a "Totalitarian State" and an open invitation for the disclosure of personal information.

The government had contended that the right to privacy of an "exclusive few" is subordinate to the right of the people to live with dignity in a developing nation. It was stated that informational privacy does not exist prior to compelling State interests and is not a fundamental right.

POST PUTTASWAMY

The decision in K.S. Puttaswamy had minimal impact on the government's thoughts or actions regarding privacy and people' personal information.

National Security vs. Privacy: The government proceeded to commission and implement mass surveillance programmes with little regard for necessity or proportionality, always citing broad national security talking points as justifications.

In July of 2018, it was revealed that the Ministry of Information and Broadcasting had issued a request for proposals for a 'Social Media Monitoring Hub,' a technical solution designed to

[13] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[14] INDIA CONST. art. 21.
[15] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[16] Kharak Singh v. State of U.P., AIR 1963 SC 1295.

monitor all social media conversations, including email. The government was forced to abandon the initiative after receiving a severe scolding from the highest court.

In August of 2018, the Unique Identification Authority of India (UIDAI), which is currently being challenged in the Supreme Court, issued a request for proposals for a similar social media surveillance scheme.

In December 2018, the Ministry of Home Affairs authorised ten Central agencies to "intercept, monitor, and decrypt any information generated, transferred, or stored on any computer in the country." This notice is currently being challenged in front of the Supreme Court.

The Income-Tax department's 'Project Insight' likewise aims to conduct mass surveillance.

The reality, however, is that with the arrival of artificial intelligence, every citizen's information is in the public domain and may be analysed. With our government's efforts to increase transparency, every information is available at the click of a mouse. With satellites and IT capabilities for global surveillance, intelligence agencies may access and analyse practically every aspect of an individual's life. In light of national security and terrorist threats, it cannot be disputed that our personal privacy is being compromised. Social networking, WhatsApp, Facebook, Twitter, and Instagram, among others, have a significant negative impact on the precious Right to Privacy.

Post-Puttaswamy, it is true that a citizen may petition the court for infringement of his fundamental right to privacy. But post-Puttaswamy, has there been a reversal in the thinking and actions of the executive? Is the right to privacy a reality for our citizens, or is it merely an embellishment of the legal books? With the proclamation of Puttaswamy verdict, has the operation of our police, which violates our Right to Liberty and Right to Privacy, changed?

Government, Parliament, and the Supreme Court should create new legislation/methodologies to strike a compromise between the right to privacy and the right to free speech. In the digital age, data is a valuable resource that should not be left unregulated.

For the protection of crimes, human rights, national security, and the fight against terrorism, the right to privacy must be subject to reasonable constraints. Five years after the Puttaswamy landmark verdict, there has been no discernible change in the attitude of law enforcement authorities, courts, the press, or the general public. This is a cause for severe concern. It is also astonishing that, to the best of my knowledge, the bench of the High Court/Supreme Court has

only cited the Puttaswamy case in 5 recorded cases in the last 5 years. Therefore, it would be foolish to expect a paradigm shift in the Right to Privacy landscape after Puttaswamy.

Although the Government has introduced Personal Data Protection Bill, 2019[17] and Information Technology Act of 2000[18], but there is no discernible change between pre- and post-Puttaswamy. In fact, the right to privacy has been further violated in the post-Puttaswamy era by the Media Trials, abusive TV debates on contemptible topics, increasing police interference, controversial social media chats, data leakages at various levels, and derogatory remarks made by politicians about their opponents. Probably, a larger awareness of the Puttaswamy dictum is required so that the common man, executive, and press have a thorough understanding of the expanded Right to Privacy and it can be respected in accordance with the dictum of the apex court.

PRIVACY AND PANDEMIC

Given the outbreak of the Covid-19 pandemic and the government's eagerness to embrace intrusive and perhaps unconstitutional technologies during these times, the principles explained in Puttaswamy are more crucial than ever for the protection of our rights. As Lord Atkin remarked in his famous opinion in the Liversidge v. Anderson[19] case, "among the clash of armaments, the laws are not silent," it is essential that any potential remedies to the difficulties caused by the epidemic be constrained by the Constitution.

The government's immunisation efforts throughout the epidemic to support their claims emphasising access and privacy concerns.

The pandemic technology violates data privacy, which leads to surveillance and exclusion. Given India's digital divide, which renders digitally-driven measures wasteful, the trade-off between privacy and pandemic technologies is unwarranted.

Such techno-solutionism can have disturbing practical ramifications. The lack of privacy policies controlling the app, the lack of clarity regarding data sharing between other apps like as Co-Win and Aarogya Setu, and how it would breach user consent if used to construct digital health IDS are the reasons for the privacy problems that plague the Co-Win platform.

[17] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, (6th December, 2019).
[18] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[19] [1941] UKHL 1.

Comparing the advantages of Digital Vaccine Certificates to traditional paper-based ones, with an emphasis on the privacy implications of their use and advice on how to make the technology more privacy-friendly.

Beyond the issues raised by the government's adoption of digital measures, further measures, such as disclosing the names of COVID-positive patients and placing notices/posters or barricades around the homes of patients, are being considered. These actions are contrary to current privacy law, notably the Puttaswamy decision.

During the pandemic, governments across the globe have adopted aggressive technology means to trace individuals and enforce quarantine, sacrificing the privacy of individuals for the possible benefit of the public health as a whole.

CONCLUSION

Being a member of society frequently trumps the notion that we are first and foremost individuals. Each person needs their own private area for whatever activity they undertake (assuming here that it shall be legal).

A rights-based data protection law that prohibits mass surveillance, establishes a judicial oversight mechanism for targeted surveillance, and recognises the principle that the government should serve as a model data controller when handling the personal information of its citizens is the need of the hour.

For the privacy judgment to fulfil its full potential, it must go beyond heated dissents and issue binding rulings that put the executive branch of government within clear, limited constitutional extremities.