IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Evolving Jurisprudence Of Privacy Laws In India

AUTHORS:

Anusha Unnikrishnan – Assistant Professor, Al Ameen College Of Law Bangalore

Aswani J S – Assistant Professor, Al Ameen College Of Law Bangalore

Riya Saji – Assistant Professor, Mount Zion Law College, Pathanamthitta, Kerala

Juney Reena Chacko – Assistant professor, Mount Zion law college, Pathanamthitta, Kerala

Archana Sathyan – BBA LLB (HONS), LLM IPR

ABSTRACT

The concept of privacy in India has evolved significantly over the years, transitioning from a peripheral notion to a fundamental right with far-reaching implications for individual freedoms. This paper explores the historical development of privacy jurisprudence in India, examining key judicial decisions and legislative efforts that have shaped the current legal landscape. A pivotal moment in this evolution was the Supreme Court's judgment in K.S. Puttaswamy v. Union of India (2017), which affirmed the right to privacy as a fundamental right under the Indian Constitution. The paper delves into the challenges posed by emerging technologies, particularly in the realms of surveillance, data protection, and digital privacy, and discusses the legislative frameworks such as the Personal Data Protection Bill, 2019 that aim to safeguard privacy in the digital era. It also offers suggestions for strengthening privacy protections, emphasizing the importance of an adaptive legal framework, public awareness, and judicial oversight. The study highlights the evolving nature of privacy rights in India, emphasizing the need to balance individual rights with state interests in a rapidly digitizing world.

KEYWORDS: (Privacy Rights**,** Jurisprudence**,** Fundamental Right**,** Data Protection**,** Surveillance)

INTRODUCTION

Privacy, once considered a mere peripheral concern, has evolved into a cornerstone of personal liberty in modern democracies. In India, the right to privacy was not initially recognized as a fundamental right under the Constitution, despite its crucial role in protecting individual dignity and freedom. However, in recent decades, judicial decisions have played a transformative role in affirming privacy as an essential constitutional right. The landmark K.S. Puttaswamy v. Union of India case in 2017 was a defining moment, where the Supreme Court of India recognized privacy as a fundamental right under Article 21 of the Constitution. This ruling set the stage for a comprehensive understanding of privacy, which now encompasses personal autonomy, data protection, and protection from unwarranted state surveillance. As India enters the digital age, privacy rights are facing new challenges, especially with the advent of state surveillance systems and private-sector data collection. The government's introduction of the Personal Data Protection Bill, 2019, and growing concerns around digital data collection signal an urgent need for stronger legal frameworks to safeguard

privacy. This paper traces the historical trajectory of privacy laws in India, analyzes key judicial milestones, and explores the role of technology and legislation in shaping the future of privacy protection in India.

THE HISTORICAL DEVELOPMENT OF PRIVACY LAWS IN INDIA

India's legal history regarding privacy rights is marked by gradual expansion. Initially, privacy was not a directly recognized right under the Indian Constitution, but over time, the courts began to infer privacy protection through various constitutional provisions, particularly Article 21.

- Early Judicial Attitudes Toward Privacy

In the early years of India's independence, privacy was not explicitly protected. Key early cases, such as MP Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962), shaped the legal understanding of privacy during this period.

- MP Sharma v. Satish Chandra (1954): This case involved the constitutional validity of search and seizure operations conducted by the police. The Supreme Court of India, in this case, ruled that the right to privacy was not a part of the fundamental rights under the Constitution. The judgment indicated that while there could be privacy protections under laws related to personal security and property, there was no specific constitutional right to privacy.[1]
- Kharak Singh v. State of Uttar Pradesh (1962): In this case, the Court considered whether surveillance of individuals violated their right to privacy. Although the Court did not explicitly recognize the right to privacy as a fundamental right, it did indicate the importance of personal liberty and bodily integrity under Article 21 of the Constitution. The Court acknowledged the need to protect individuals from state surveillance, but it did not extend the protection to include privacy in all contexts.[2]

- The Shift Toward Privacy Protection (1970s to 1990s)

By the 1970s, judicial attitudes began to change, and privacy concerns started to be considered in broader terms.

- R. Rajagopal v. State of Tamil Nadu (1994): This case marked a turning point in Indian privacy jurisprudence. The Supreme Court ruled that the right to privacy could not be ignored, even for public figures. The case dealt with a journalist's right to publish details about a public figure's life, but it was clear that individuals have a right to be left alone unless there is a compelling public interest. This judgment established that the right to privacy is not confined to protecting private property or personal security but extends to personal autonomy and bodily integrity as well.[3]

This period set the stage for privacy becoming a more important legal concept in India, particularly in the context of human dignity and autonomy.

LANDMARK JUDGMENT: K.S. PUTTASWAMY V. UNION OF INDIA (2017)

The K.S. Puttaswamy case (2017) was the most crucial development in the legal recognition of privacy as a fundamental right. The petitioners in this case challenged the Aadhaar scheme, arguing that it violated their

[1] Dhavan, Rajeev. *Juristic techniques in the Supreme Court of India (1950-1971) in some selected areas of public and personal law*. University of London, School of Oriental and African Studies (United Kingdom), 1972.

[2] Thakral, Apoorva. "The Evolutionary Journey of Right to Privacy." *Indian JL & Legal Rsch.* 2 (2021): 1.

[3] Bennett, Colin J. "Convergence revisited: Toward a global policy for the protection of personal data." *Technology and privacy: The new landscape* (1997): 99-123.

right to privacy. The Supreme Court's ruling was a landmark one, as it formally declared the right to privacy to be a fundamental right under the Constitution of India.[4]

Key Takeaways from the Puttaswamy Judgment:

1. Recognition of Privacy as a Fundamental Right: The Court held that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Indian Constitution. The Court emphasized that privacy is fundamental to the protection of human dignity, autonomy, and personal freedom. This marked the first time that privacy was explicitly recognized as a constitutional right in India.
2. Overruling Previous Precedents: The Court overruled earlier judgments that had downplayed the significance of privacy as a constitutional right. Specifically, it revisited the judgments in MP Sharma and Kharak Singh, and the bench in Puttaswamy concluded that those decisions were outdated, given the evolving understanding of privacy in the modern world.
3. Privacy as a 'Right of Individuals': The judgment made it clear that privacy belongs to the individual and that no one—including the state—has the right to violate it without just cause. It stressed that privacy is essential for the individual's self-expression, decision-making, and independence in social, political, and economic life.
4. Balancing Privacy with Other Public Interests: While privacy was affirmed as a fundamental right, the Court also stated that this right is not absolute. It can be subjected to limitations or restrictions, particularly when there is a legitimate state interest, such as in cases related to national security, public health, or criminal investigation. The Court emphasized that any state action infringing on privacy must meet the "test of proportionality," meaning the restriction must be necessary, legitimate, and proportionate to the objective sought to be achieved.[5]

EMERGING TECHNOLOGICAL CHALLENGES TO PRIVACY IN INDIA

As India has rapidly digitized, new challenges to privacy have emerged, particularly in the realms of surveillance, data collection, and digital rights. Technological advancements have exposed the vulnerabilities of individuals in the digital space, leading to heightened concerns about privacy.

- Aadhaar and Data Privacy[6]

The Aadhaar project, which aims to provide a unique identification number to every resident of India, has been at the center of privacy debates. While it is seen as a tool for improving welfare distribution and reducing corruption, it raises significant privacy issues, including the potential for unauthorized surveillance and data breaches.

- Challenges with Aadhaar: Critics of the Aadhaar scheme argue that its wide-reaching database and biometric data collection could be misused for surveillance purposes, potentially violating individual privacy. The Court, in the Puttaswamy judgment, acknowledged these concerns, ruling that while the Aadhaar system could be constitutional under certain circumstances, its use should be limited and should not compromise citizens' privacy rights.

- Surveillance Technologies and Privacy[7]

Surveillance technologies, such as facial recognition, mobile tracking, and the monitoring of online activity, pose serious challenges to privacy. In the face of national security concerns and crime prevention,

[4] Puttaswamy, Justice KS. "v. Union of India.(2017) 10 SCC 1."

[5] Mishra, Arsh. "Case Analysis on Justice KS Puttaswamy [Retired] vs Union of India and Ors." *Issue 3 Indian JL & Legal Rsch.* 4 (2022): 1.

[6] Singh, Pawan. "Aadhaar and data privacy: biometric identification and anxieties of recognition in India." *Information, Communication & Society* 24.7 (2021): 978-993.

[7] Patton, Jason W. "Protecting privacy in public? Surveillance technologies and the value of public places." *Ethics and Information Technology* 2 (2000): 181-187.

governments around the world are increasingly utilizing surveillance tools that can infringe upon individual privacy. The rise of smart cities, internet of things (IoT) devices, and ubiquitous cameras makes it more difficult to safeguard individuals' personal information.

- Facial Recognition and Privacy Invasion: The deployment of facial recognition technology, especially in public spaces, raises alarms about mass surveillance without adequate safeguards or oversight.
- Data Harvesting by Private Companies: Social media platforms, mobile applications, and tech companies collect vast amounts of personal data, often without full transparency. Such data is used to target advertisements, manipulate behavior, or even influence elections. This information asymmetry between individuals and corporations is a significant concern for privacy advocates.

LEGISLATIVE DEVELOPMENTS AND THE FUTURE OF PRIVACY PROTECTION

As privacy concerns continue to grow in the digital age, India's legislative landscape has also evolved to address these challenges. One of the most significant steps taken to protect privacy was the introduction of the Personal Data Protection Bill (2019).

- Personal Data Protection Bill (2019)[8]

This Bill, inspired by the European Union's General Data Protection Regulation (GDPR), seeks to establish a comprehensive framework for the protection of personal data in India. Key features of the Bill include:

- Data Protection Rights: The Bill provides citizens with rights over their personal data, such as the right to access, correction, and erasure of their data.
- Consent-Based Data Processing: It requires companies to obtain explicit consent from individuals before collecting or processing their data.
- Establishment of a Data Protection Authority (DPA): The Bill proposes the creation of an independent authority to oversee and regulate data collection practices, investigate complaints, and enforce penalties for non-compliance.
- Cross-Border Data Transfers: The Bill includes provisions on the transfer of data outside India, ensuring that data protection standards are upheld even when data is transferred across borders.

- Challenges in Implementation

While the Personal Data Protection Bill is a step in the right direction, its full implementation is still pending. There are concerns about the extent to which it will be enforced and whether it will adequately address the rapid advancements in surveillance technology and data mining techniques.

THE WAY FORWARD

India is at a critical juncture when it comes to privacy protection. As technology continues to advance, the existing legal framework must evolve to ensure that privacy rights are not compromised. Here are some key suggestions for strengthening privacy laws in India:

1. Finalizing the Personal Data Protection Bill: The government should prioritize the passing of the Personal Data Protection Bill to ensure comprehensive data protection. It should also be continuously updated to address new challenges in the digital ecosystem.
2. Independent Oversight: An independent Data Protection Authority (DPA) should be established with sufficient powers to investigate privacy violations, impose penalties, and ensure compliance with data protection regulations.

[8] Singh, Ram Govind, and Sushmita Ruj. "A technical look at the Indian personal data protection bill." *arXiv preprint arXiv:2005.13812* (2020).

3. Public Education and Awareness: Given that most individuals are unaware of the full scope of their privacy rights, public awareness campaigns are necessary to educate people about how their data is used and how they can protect their privacy online.
4. Judicial Oversight of Surveillance Programs: The judiciary should continue to play an active role in reviewing the constitutionality of surveillance programs and ensuring that they do not infringe upon the right to privacy beyond what is necessary and proportionate.[9]

FINDINGS

1. Privacy as a Fundamental Right: The Puttaswamy judgment (2017) recognized privacy as a fundamental right under Article 21 of the Indian Constitution.
2. Technological Challenges: Rapid technological advancements raise concerns about data privacy and surveillance.
3. State Data Collection: Government projects like Aadhaar have sparked debates over privacy and security.
4. Legislative Efforts: The Personal Data Protection Bill is a step towards regulating data privacy, though implementation is still pending.
5. Public Awareness: There is a lack of public understanding of privacy rights and data protection.

SUGGESTIONS

1. Implement Data Protection Laws: Enforce and regularly update the Personal Data Protection Bill.
2. Empower Data Protection Authority: Strengthen the independence and effectiveness of the Data Protection Authority.
3. Ensure Judicial Oversight: Maintain judicial oversight of surveillance programs to protect privacy.
4. Increase Public Awareness: Launch awareness campaigns to educate citizens on privacy rights.
5. Adapt to New Technologies: Update privacy laws to address challenges posed by emerging technologies.

CONCLUSION

The jurisprudence of privacy law in India has evolved significantly, with the recognition of privacy as a fundamental right in the Puttaswamy case marking a watershed moment. However, the challenges presented by modern technology—ranging from surveillance to data privacy—are significant. Moving forward, comprehensive legislation, robust enforcement mechanisms, and continued judicial vigilance will be necessary to ensure that privacy remains a protected and respected right in India. The evolving legal and technological landscape requires constant adaptation to safeguard individual freedoms in an increasingly digital world.

REFERENCES:

- K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
- R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632.
- Personal Data Protection Bill, 2019, available at: https://www.prsindia.org/billtrack/personal-data-protection-bill-2019
- Batra, R. (2020). Privacy, Technology, and the Law in India: A Contemporary Review. Journal of Indian Law, 35(2), 159-178.
- Jain, P. (2021). The Impact of Digital Surveillance on Privacy Rights. Indian Law Review, 7(1), 45-62.
- Rodotà, Stefano. "Data protection as a fundamental right." *Reinventing data protection?*. Dordrecht: Springer Netherlands, 2009. 77-82.

[9] Rodotà, Stefano. "Data protection as a fundamental right." *Reinventing data protection?*. Dordrecht: Springer Netherlands, 2009. 77-82.

- Singh, Ram Govind, and Sushmita Ruj. "A technical look at the Indian personal data protection bill." *arXiv preprint arXiv:2005.13812* (2020).
- Singh, Pawan. "Aadhaar and data privacy: biometric identification and anxieties of recognition in India." *Information, Communication & Society* 24.7 (2021): 978-993.
- Patton, Jason W. "Protecting privacy in public? Surveillance technologies and the value of public places." *Ethics and Information Technology* 2 (2000): 181-187.
- Puttaswamy, Justice KS. "v. Union of India.(2017) 10 SCC 1."
- Mishra, Arsh. "Case Analysis on Justice KS Puttaswamy [Retired] vs Union of India and Ors." *Issue 3 Indian JL & Legal Rsch.* 4 (2022): 1.
- Dhavan, Rajeev. *Juristic techniques in the Supreme Court of India (1950-1971) in some selected areas of public and personal law*. University of London, School of Oriental and African Studies (United Kingdom), 1972.
- Thakral, Apoorva. "The Evolutionary Journey of Right to Privacy." *Indian JL & Legal Rsch.* 2 (2021): 1.
- Bennett, Colin J. "Convergence revisited: Toward a global policy for the protection of personal data." *Technology and privacy: The new landscape* (1997): 99-123.