



INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed Edition :

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

IJLRA

EDITORIAL TEAM

EDITORS

Megha Middha



Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmanagarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmanagarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8 Articles in various reputed Law Journals. Conducted 1 Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-I, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC - NET examination and has been awarded ICSSR - Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

EVOLUTION OF RIGHT TO PRIVACY AS FUNDAMENTAL RIGHT

AUTHORED BY - ASHISH CHANDELA

A3211119361

B.A LL.B(H)

AMITY LAW SCHOOL, NOIDA AMITY UNIVERSITY

LIST OF CASES

<i>Name of Case</i>
Prince Albert v. Strange (1849)
Roberson v. Rochester Folding Box Co. (1902)
Olmstead v. United States (1928)
Griswold v. Connecticut
Roe v. Wade (1973)
Gobind v. State of Madhya Pradesh (1975)
K.S. Puttaswamy v. Union of India (2017)
Selvi v. State of Karnataka (2010)

ABSTRACT

This research explores the evolution of the right to privacy as a fundamental right in India, set against a backdrop of both national and global legal landscapes. The importance of privacy as a fundamental right has grown significantly, reflecting its crucial role in modern democratic societies. Through a comprehensive legal doctrinal approach, comparative analysis, and detailed case law review, this study delves into the transformation and current challenges of privacy rights within the Indian context, while also drawing comparisons with international jurisdictions.

The research begins with a historical overview that traces the global evolution of privacy rights alongside India's own journey from traditional cultural interpretations to formal legal recognition. Key legal developments, policies, and legislative measures that have influenced privacy rights in India are discussed, providing a foundational understanding of the shift in privacy perspectives over the years. The core of the study focuses on the constitutional framework of privacy in India. By analyzing constitutional provisions, early debates from the Constituent Assembly, and subsequent judicial interpretations, the research highlights how the Indian judiciary has played a pivotal role in shaping privacy as a fundamental right, culminating in the landmark judgment of Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017), which officially recognized privacy as part of the fundamental rights under the Indian Constitution.

A comparative analysis with jurisdictions such as the USA, the EU, and other Asian countries is conducted to identify best practices and potential improvements for India. This includes an examination of the General Data Protection Regulation (GDPR) in Europe and the Fourth Amendment in the USA. The study also addresses the contemporary challenges posed by digital advancements and surveillance, scrutinizing the balance between privacy and technology. It concludes with a set of recommendations aimed at strengthening privacy protection in India and suggests future research directions to continue enriching the discourse on privacy rights, ensuring their adaptation and resilience in the digital age.

Right To Privacy As fundamental Right

The right to privacy, recognized globally as a cornerstone of individual autonomy and personal freedom, assumes paramount importance in our increasingly interconnected 21st-century world. Stemming from the desire for solitude and the right to control personal information, the right to privacy serves as a bulwark against unwanted intrusions by the state, organizations, or other

individuals. This fundamental right is not only a legal shield but also a crucial component of the social fabric that underpins democratic governance and the respect for human dignity.

From a legal perspective, the right to privacy is enshrined in numerous international human rights treaties and national constitutions around the world. It is articulated in Article 12 of the Universal Declaration of Human Rights and elaborated upon in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which imposes on states the obligation to protect individuals against "arbitrary or unlawful interference" with their privacy. Many countries have interpreted this through their judicial systems to adapt to the evolving nature of privacy, recognizing it not merely as a right to be left alone but also encompassing a broader range of personal rights, including bodily integrity, protection of personal data, and freedom from surveillance. In the context of India, the Supreme Court's landmark decision in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017) emphatically recognized privacy as a fundamental right under the Constitution. This ruling not only reaffirmed the significance of privacy in the face of modern challenges but also underscored its intrinsic link to the exercise of other fundamental rights, such as freedom of speech, movement, and peaceful assembly. The judgment is a testament to the dynamic interpretation of constitutional rights, reflecting societal values that evolve over time.

The significance of privacy in the 21st century can be viewed through both legal and social lenses, especially as digital technology continues to permeate all aspects of human life. Legally, the right to privacy underpins the development of laws and policies concerning data protection, which are crucial in the digital age. For instance, the General Data Protection Regulation (GDPR) in the European Union and various data protection laws across the world are designed to give individuals control over their personal data, thereby enhancing their privacy rights. These laws regulate how personal information is collected, stored, processed, and shared, reflecting the legal recognition of privacy as a fundamental right that must be protected in both public and private spheres. Socially, the concept of privacy has undergone a significant transformation, influenced largely by technological advancements. The proliferation of digital devices and the internet has blurred the lines between public and private life. Social media platforms, where individuals voluntarily share vast amounts of personal information, present new challenges to the traditional understanding of privacy. The right to privacy in such a context involves navigating the delicate balance between sharing and protecting personal information. It also raises critical questions about consent, the permanence of online activities, and the right to be forgotten, which have significant implications for personal reputation and psychological well-being.

Moreover, the surveillance capabilities of modern technology pose unprecedented challenges to privacy. Governments and corporations have the tools to track and analyze individual behavior on a scale previously unimaginable. This surveillance, while often justified on grounds of security or economic benefit, raises profound questions about the limits of state power and corporate responsibility. It underscores the need for robust legal frameworks that govern surveillance practices, ensuring that they do not encroach unduly on individual rights. The discourse on privacy also intersects with other critical issues of the 21st century, such as inequality and discrimination. Marginalized and vulnerable groups often face disproportionate privacy invasions, both from state and non-state actors. The protection of privacy, therefore, is also a question of social justice, requiring legal and societal efforts to ensure that privacy rights are respected universally and equitably.

The nexus between the right to privacy as a basic human right and its recognition as a fundamental right is a critical intersection in the realm of legal jurisprudence and human rights discourse. This convergence reflects the universal acceptance and essential nature of privacy rights, underscoring their foundational role in upholding human dignity and autonomy across diverse legal systems.

Privacy as a basic human right is recognized internationally, rooted in the notion that all individuals deserve a sphere of personal autonomy free from undue interference. This concept is articulated in major international human rights instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), which assert the right to privacy as a fundamental aspect of human dignity and freedom. These documents provide a normative framework that guides nations in adopting and implementing laws to protect privacy. However, the interpretation and application of these rights can vary significantly based on cultural, social, and legal contexts, which is where the designation as a fundamental right becomes pivotal. The designation of privacy as a fundamental right within national constitutions or legal frameworks elevates its status, providing it with a heightened level of protection. This classification means that privacy is not just a legal standard, but a core value that is essential to the functioning of a free and democratic society. In jurisdictions where privacy is recognized as a fundamental right, any infringement by the state or other entities must meet a higher standard of justification, typically under strict scrutiny standards. This involves proving that any encroachment is necessary for a compelling state interest and is executed in the least invasive manner possible.

In countries like India, the Supreme Court's landmark decision in Justice K.S. Puttaswamy (Retd.)

vs. Union of India (2017) underscored this nexus by declaring privacy as a fundamental right protected under the Indian Constitution. This decision was not merely a recognition of privacy in isolation but was deeply interconnected with other fundamental rights such as freedom of speech, freedom of movement, and the right to life. By situating privacy within this framework, the Court emphasized that a violation of privacy could lead to violations of other critical rights, illustrating the inherent interconnectedness of human rights. This acknowledgment of privacy as a fundamental right addresses several contemporary challenges, particularly in the digital age where data breaches, surveillance, and loss of confidentiality are prevalent. As technology evolves, so does the potential for intrusion into the private lives of individuals. Recognizing privacy as a fundamental right ensures that laws and policies governing the use of technology not only keep pace with innovations but are also rooted in the protection of individual autonomy and respect for personal data.

Moreover, the nexus between privacy as a human right and a fundamental right has significant implications for governance and the rule of law. It acts as a check on state power, limiting how governments can collect and use personal information. This is crucial in preventing abuses such as unwarranted surveillance, which can stifle free expression and suppress dissent. In democracies, upholding privacy as a fundamental right is synonymous with protecting the freedoms that form the bedrock of democratic governance.

From a social perspective, this nexus supports societal development by fostering a sense of security that individuals feel when they know their private information is protected. This, in turn, encourages participation in social, economic, and political activities, contributing to a more engaged and active citizenry. Privacy, thus, supports not only individual development but also the collective advancement of society. Internationally, the recognition of privacy as a fundamental right also influences global norms and practices. It sets a benchmark that can inspire legal reforms in other countries, promoting a broader international commitment to upholding privacy. This global perspective is increasingly important in an interconnected world where cross-border data flows and international cooperation are routine.

CONCLUSION

The intricate journey of understanding and evolving the right to privacy as a fundamental right reflects a profound recognition of individual autonomy and the inherent need for personal space

in our increasingly digital society. As the research has illuminated, privacy is not a static concept but a dynamic right that has undergone substantial transformation, particularly in the context of technological advancements and changing societal norms. From its origins in the protection against physical intrusions to its current interpretation that encompasses digital privacy, the right to privacy has continuously expanded to address new challenges and scenarios. In India, the landmark ruling in Justice K.S. Puttaswamy (Retd.) vs. Union of India is a testament to the judiciary's role in not only recognizing but also fortifying privacy as a constitutional right. This decision has catalyzed a re-evaluation of various laws and policies, ensuring that they align with the fundamental rights guaranteed by the Constitution. The case marked a pivotal moment, highlighting the necessity of privacy protections in the age of information, where data has become both a resource and a potential point of vulnerability.

The global perspective on privacy rights, as analyzed through comparative studies, shows a wide array of protections and frameworks, from the stringent GDPR in the European Union to more nascent privacy laws in other parts of the world. These variations underscore the influence of cultural, economic, and political factors on the implementation and enforcement of privacy laws. However, the common thread across all jurisdictions is the acknowledgment of privacy as an essential component of human dignity and freedom. Technological advancements, while beneficial in countless ways, have presented unprecedented challenges to privacy. The proliferation of digital data and the capabilities for surveillance have outpaced the legal frameworks designed to manage them. This disjunction necessitates a continuous reevaluation of privacy laws to ensure they are robust enough to handle the nuances of digital data management and the capabilities of modern technology. The discussions around digital privacy and surveillance have shown that while technology can facilitate the infringement of privacy, it can also be harnessed to protect it through enhanced security measures and encryption technologies.

Socially, the recognition of privacy as a fundamental right plays a crucial role in maintaining democratic values. It supports the free expression and autonomy of individuals, enabling them to participate fully in society without undue interference. In this regard, privacy is closely linked to other fundamental rights, such as freedom of speech and freedom of association, creating a holistic framework that supports a free and open society. Legally, the establishment of privacy as a fundamental right provides a higher threshold for any governmental or private actions that might infringe upon it. This legal protection is crucial in holding entities accountable and ensuring that any breach of privacy must be justified by a legitimate and compelling state interest, applied in the

least intrusive manner possible. The ongoing legal debates and court decisions continue to shape the contours of what constitutes a permissible intrusion into personal privacy, balancing state and corporate interests against individual rights.

The challenges highlighted throughout this research—ranging from government surveillance to private data breaches—illustrate the complexities involved in protecting privacy in a digital age. These issues are not confined to any single nation but are part of a global discourse on how to effectively safeguard personal information in a world where data flows across borders with ease. Therefore, international cooperation and harmonization of privacy standards are essential to address these challenges effectively. As we look to the future, the trajectory of privacy laws will likely need to incorporate a more nuanced understanding of technological impacts and ethical considerations. The right to privacy will continue to evolve, and legal frameworks will need to be both flexible and resilient to adapt to future technological innovations. Areas such as artificial intelligence, big data analytics, and the Internet of Things will test the limits of current privacy laws and demand innovative legal responses.

The evolution of privacy as a fundamental right, particularly in the digital age, poses several complex challenges that necessitate robust and adaptable policy interventions. As we delve deeper into a world dominated by digital interactions and data transactions, the need for comprehensive, clear, and effective privacy policies becomes paramount. Based on the research and analysis conducted, several policy recommendations emerge as critical measures to safeguard privacy in contemporary society.

Firstly, there is a pressing need to update and harmonize privacy legislation to reflect the realities of digital technology and data flows. Current laws often lag behind technological advancements, leaving gaps that can be exploited to infringe on individual privacy. Policymakers should ensure that privacy laws are technology-agnostic, flexible enough to adapt to new technologies, and stringent enough to provide real protection. This includes the creation of standards for data minimization, where only the necessary amount of personal data is collected, and data retention policies that dictate the secure deletion of data once it is no longer needed for the purpose it was collected. Secondly, transparency and accountability must be embedded into the operations of both public and private entities that handle personal data. This can be achieved through stringent requirements for data controllers and processors to disclose their data handling practices and undergo regular audits. The implementation of privacy impact assessments before deploying new

technologies or data practices can help identify potential privacy issues before they arise. Furthermore, these entities should be obligated to report data breaches promptly to both regulators and the affected individuals, ensuring that all parties are informed and can take necessary actions to mitigate the impact.

Thirdly, there is a crucial need for stronger enforcement mechanisms. While many jurisdictions have privacy laws in place, their enforcement is often weak or inconsistent. Regulatory bodies should be empowered and adequately funded to enforce privacy laws effectively. This includes having the authority to impose significant penalties on those who violate privacy rights to deter non-compliance. Additionally, the establishment of specialized courts or tribunals to handle privacy disputes could provide the expertise needed to deal with complex cases involving technology and data. Fourthly, the right to privacy must be balanced with other societal interests, such as national security and public safety. However, this balance should not be skewed disproportionately against privacy. Policies should therefore establish clear, narrow, and specific criteria under which exceptions to privacy rights may be allowed, and these exceptions should be subject to strict oversight. Measures such as judicial warrants for surveillance activities can provide a necessary check on the powers of the state.

Fifthly, the global nature of data flows necessitates international cooperation in privacy protection. Policies should encourage the development of international standards and agreements that facilitate cross-border data protection while respecting the sovereignty and legal frameworks of participating countries. This could be facilitated by adopting frameworks similar to the EU's General Data Protection Regulation (GDPR), which not only standardizes data protection across EU members but also affects how data is handled between the EU and other nations.

Sixthly, there should be an increased focus on public education and awareness about privacy rights and data protection. Many data breaches and privacy violations occur due to a lack of knowledge or careless behavior by individuals in handling their personal information. Governments, in partnership with educational institutions and civil society, should develop comprehensive digital literacy programs that educate citizens of all ages about the importance of privacy and the steps they can take to protect their personal information.

Seventhly, specific attention should be given to the development of ethical guidelines for emerging technologies such as artificial intelligence (AI) and big data analytics. These guidelines should

ensure that innovations respect privacy rights and ethical considerations are integrated into the development and deployment stages of technological solutions. This includes ethical data sourcing, bias mitigation in AI algorithms, and ensuring that automated decisions are transparent and accountable. Finally, recognizing the unique challenges faced by vulnerable populations in protecting their privacy, policies should ensure that privacy protections are inclusive and accessible to all individuals. This includes adapting privacy protections to be understandable and usable across different languages and cultural contexts, as well as providing special safeguards for data concerning minors and other vulnerable groups.

In conclusion, advancing the right to privacy in the 21st century requires a multifaceted approach that includes legal reform, enforcement enhancements, international cooperation, public education, and the ethical development of technology. By adopting these policy recommendations, governments and organizations can help ensure that privacy is protected as both a fundamental and functional right in the digital era, thus fostering trust and security in the digital infrastructure that increasingly underpins our social and economic activities.

