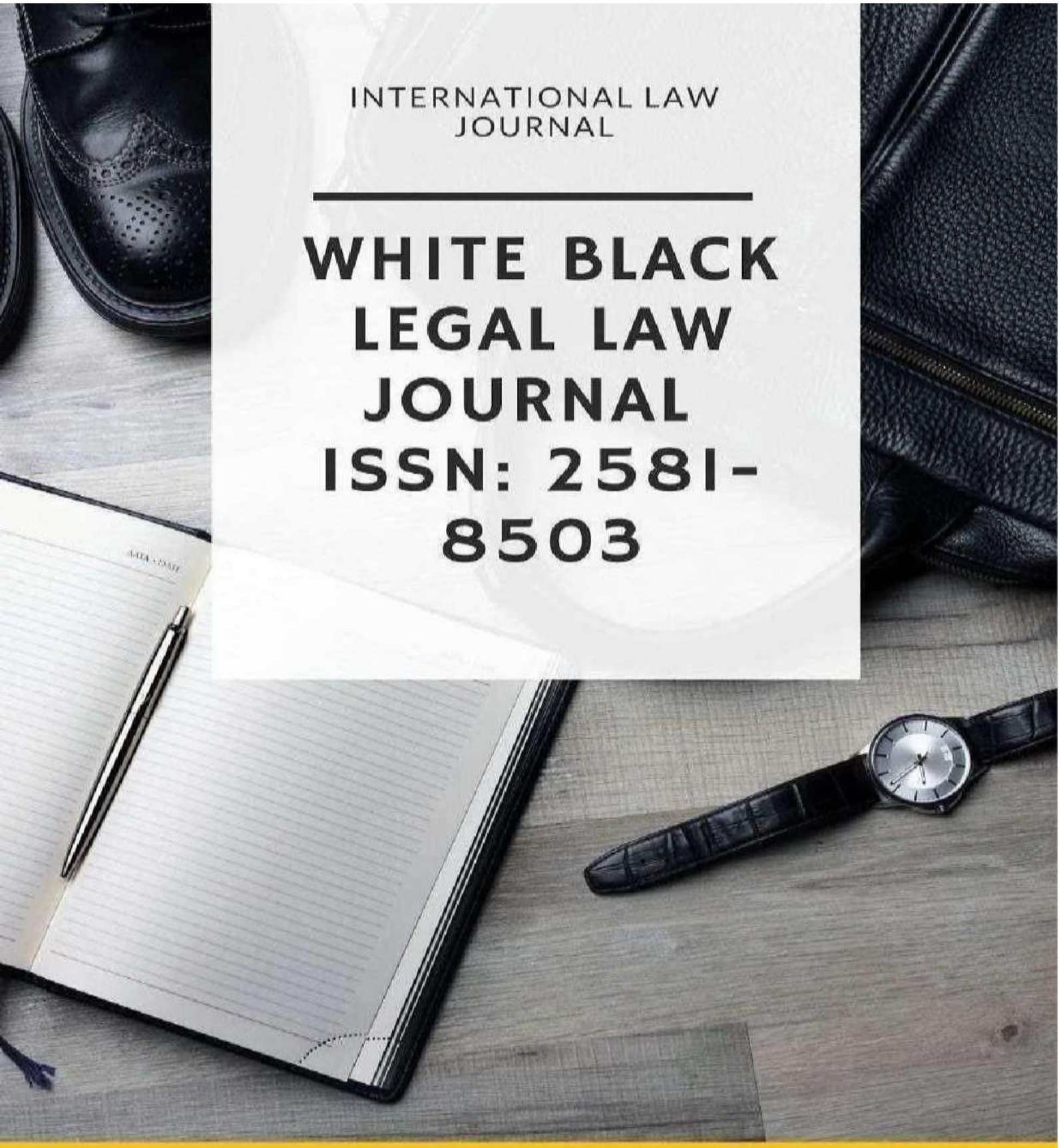

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

THE RIGHT TO PRIVACY VS MASS SURVEILLANCE: A LEGAL AND ETHICAL ANALYSIS IN THE AGE OF GLOBAL SECURITY CONCERNS.[1]

AUTHORED BY - BHUVANESHWARI. M & GAYATHRI. A

Abstract

The Right to Privacy and the mass surveillance are critical issues in the modern legal and ethical debates, especially with the rise of digital technologies such as social media, public health concerns, national security concerns etc. The Right to Privacy is recognized as a fundamental right under Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty, it stressed that privacy constitutes an integral component of the right to life and personal liberty. Whereas, on the other hand, Mass surveillance refers to the systematic monitoring of a significant segment of a population, typically conducted by government entities or private corporations for the purpose of protecting national security, to prevent crime and to fight terrorism. In this research paper, the doctrinal method of study has been implemented for finding the ways to balance these two competing interests. The conflict between these two interests has grown increasingly prominent in the recent years, with the rise of modern days issues such as data privacy, government surveillance, and freedom of expression as global discussions. Though both the interests are conflicting with each other, the Right to Privacy is a fundamental right but not absolute and subject to reasonable restrictions. Similarly, Mass Surveillance is not a right under International law as well as Indian law and it often involves invasive data collection, which can conflict with the Right to Privacy. This paper aims to critically analyze how to achieve the harmony between the Right to Privacy and Mass Surveillance guided by the principles of necessity, proportionality, accountability and public safety and it further ensures that governance protects the national security without undermining individuals' fundamental rights.

Keywords: Transparency, Personal Data, Data Privacy, National Security, Surveillance Democracy.

[1] BHUVANESHWARI. M – ASSISTANT PROFESSOR, VISTAS
GAYATHRI. A – ASSISTANT, VISTAS

1. INTRODUCTION

In India, the Right To Privacy (RTP) is recognized as a fundamental right and is safeguarded under the Constitution of India, 1950. Though the Indian Constitution did not explicitly mention a "right to privacy." However, Articles 19[2] and 21[3] have been interpreted as providing a basis for the right to privacy. The right to privacy is a vital component of personal liberty and dignity, encompassing the freedom to be left undisturbed, make independent decisions regarding personal matters, and safeguard personal data from misuse or exploitation. The right to privacy is not an absolute right and may be subject to reasonable restrictions. Any state action limiting this right must be backed by a legislative mandate, serve a legitimate state objective, and comply with the principle of proportionality. This means the restriction must be necessary in a democratic society and implemented through the least intrusive means available. The right to privacy encompasses personal information, communication, decision-making, movements, personal choices, relationships, and eating habits. The first case to address the right to privacy in India was **Kharak Singh v. State of Uttar Pradesh**[4], it was a landmark judgment in the evolution of the right to privacy in India. Although the Supreme Court did not explicitly recognize privacy as a fundamental right, the case laid the groundwork for future developments in this area. The Supreme Court delivered a split verdict addressing the constitutionality of police surveillance to the suspect of the robbery case. It upheld general surveillance practices like shadowing, stating they did not infringe fundamental rights unless they involved physical restraint. However, domiciliary visits were declared unconstitutional as they violated personal liberty under Article 21. While the majority, led by Ayyangar J denied that "personal liberty" was confined to "freedom from physical restraint or freedom from confinement within the bounds of a prison" and held that 'personal liberty' was used in the article as a compendious term to include within itself all the varieties of rights which go to make up the "personal liberties" of a human being other than those deal with the several clauses of Article 19 (1)[5]. He further held that the right to privacy was not explicitly guaranteed as a fundamental right under the Constitution. Justice Subba Rao's dissent recognized privacy as inherent to personal liberty under Article 21, asserting that unauthorized intrusion into one's home undermines dignity and liberty. Although the Court acknowledged that personal liberty

[2] Art 19. (1) All citizens shall have the right—(a) to freedom of speech and expression;
[3] Art 21. No person shall be deprived of his life or personal liberty except according to procedure established by law.
[4] 1963 AIR 1295
[5] V. N Shukla, *Constitution of India* (EBC, 13th edn.).

under Article 21 protects against unjustified intrusions, it refrained from explicitly recognizing privacy as a standalone right.

The Right to Privacy (RTP) is a legally enshrined principle that safeguards individuals against both governmental and private intrusions into their personal sphere. It is acknowledged in various International legal instruments. Moreover, it is explicitly referenced or implied in the constitutional frameworks of over 185 nations worldwide, which will be discussed in this research paper.

Whereas, Mass surveillance refers to the extensive monitoring of an entire population or a significant portion of it to observe and track their activities. This surveillance is typically conducted by local or federal governments and their agencies, but it can also be carried out by corporations, either on behalf of governments or independently for their own purposes. The legality of mass surveillance depends on a country's legal framework, constitutional protections, and international human rights obligations. Mass surveillance involves the large-scale collection and monitoring of individuals' data, communications, and activities, often by state agencies. Its legality is often debated due to its potential conflict with fundamental rights such as privacy, freedom of expression, and freedom of movement.

In India, mass surveillance is legal under specific conditions, similar to certain countries, including those in the European Union. The Indian Telegraph Act of 1885 is one of the key laws that facilitates the surveillance of electronic communications in contemporary India. Further, several other statutory provisions in India also address mass surveillance such as the Information Technology Act, 2000, the Code of Criminal Procedure (CrPC), 1973, etc,. Though Mass Surveillance helps with preventing crimes and other forms of violations, it frequently conflicts with the right to privacy, as recognized under Article 21 of the Indian Constitution and international frameworks such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR). Furthermore, the UN General Assembly has passed the **Resolution 68/167**, adopted in December 2013 emphasizing the need to protect privacy in the digital age, condemning mass surveillance that violates international law. The UN Human Rights Committee stresses that surveillance must meet the tests of legality, necessity, and proportionality.

THE NEED AND IMPORTANCE OF RIGHT TO PRIVACY

The Right to Privacy is essential for safeguarding individual dignity, autonomy, and freedom in a democratic society. It allows individuals to make decisions about their personal lives without undue interference, including choices related to family, relationships, reproductive rights,etc,. and thereby ensuring respect for personal autonomy. Privacy is closely tied to human dignity, enabling individuals to maintain control over their personal information, thoughts, and actions, and protecting them from intrusions that could lead to humiliation or a loss of self-respect. It acts as a check on state power, preventing arbitrary or excessive surveillance and preserving democratic freedoms while guarding against authoritarianism.

In the digital age, where personal data is constantly collected and processed by governments and corporations, privacy becomes crucial in protecting individuals from the misuse of their data, such as identity theft, profiling, and discrimination. It fosters freedom of thought and expression[6] by creating a safe space for individuals to think freely, express opinions, and engage in discourse without fear of reprisal or censorship. Privacy also provides critical protection for marginalized groups, shielding them from exploitation, harassment, and targeted surveillance, while ensuring fair practices in the digital economy by preventing unauthorized use of personal data for profit or manipulation. Moreover, it safeguards sensitive health information, allowing individuals to seek medical care or counseling without fear of exposure or stigma. Ultimately, the Right to Privacy is a cornerstone of individual freedom and democracy, ensuring that people can live with dignity, security, and autonomy while maintaining a balanced relationship between citizens, the state, and private entities in the modern age.

The Right to Privacy in India, though not explicitly mentioned as a fundamental right in the original Constitution, it has been recognized as an integral part of the Right to Life and Personal Liberty under Article 21. This recognition has evolved through judicial interpretation over the years, with significant milestones in the Indian legal landscape. Article 21 guarantees that “No person shall be deprived of his life or personal liberty except according to the procedure established by law,” and the judiciary has expansively interpreted “personal liberty” to include privacy. Additionally, though the word “privacy” is not explicitly mentioned, the principles of liberty, dignity, and freedom enshrined in the Preamble, along with Articles 14 (Right to

[6] Art 19 (1)(a) to freedom of speech and expression

Equality) and 19 (Freedom of Speech and Expression), reinforce privacy as a constitutional value.

THE HISTORY OF RIGHT TO PRIVACY

The history of the Right to Privacy (RTP) in India dates back to the Constitution of India Bill, 1895, which stated, "Every citizen has in his house an inviolable asylum." This notion evolved through various stages, including the Commonwealth of India Bill, 1925, which declared, "Every person shall have the fundamental right to liberty of person and security of his dwelling and property." Although the concept of privacy was not explicitly discussed during the Constituent Assembly debates, the protection of personal liberties was gradually incorporated into India's constitutional framework.

The Nehru (Swaraj) Report, 1928, emphasized that, "No person shall be deprived of his liberty nor shall his dwelling or property be entered, sequestered, or confiscated save in accordance with the law," reflecting a growing commitment to personal freedoms and privacy.

RTP IN THE CONSTITUTIONAL ASSEMBLY

During the Constituent Assembly, several prominent members expressed their views on the protection of personal privacy:

- K.T. Shah's Note on Fundamental Rights (Dec. 1946) advocated for the security of individuals' persons, papers, property, and homes against unreasonable search or seizure.
- K.M. Munshi's Note on Fundamental Rights (Mar. 1947) emphasized the right to the inviolability of one's home, the secrecy of correspondence, and protection from family interference.
- Harnam Singh's Note on Fundamental Rights (Mar. 1947) further asserted that every dwelling should be inviolable, drawing inspiration from the Czech Constitution.
- Dr. Babasaheb Ambedkar's Memo on Fundamental Rights (Mar. 1947) proposed that people's rights to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures should be upheld, with warrants issued only on probable cause and clear specification of the place to be searched. These early debates and proposals laid the groundwork for the eventual incorporation of the RTP in India's constitutional jurisprudence.

AN EVOLUTION OF RIGHT TO PRIVACY THROUGH JUDICIAL INTERPRETATION

As mentioned above, in *Kharak Singh's case*, Justice Subba Rao, in his minority opinion, held that the Right to Privacy is "an essential ingredient of personal liberty." He emphasized that personal liberty includes the right of an individual to be free from restrictions or encroachments on their person, whether those restrictions are directly imposed or indirectly brought about through calculated measures. Applying this principle, he found the entire regulation in question violation of Article 21, which protects the right to life and personal liberty, as well as Article 19(1)(a), which guarantees the freedom of speech and expression, and Article 19(1)(d), which ensures the right to move freely throughout the territory of India.

In *Gobind v. State of Madhya Pradesh*[7], the court considered the possibility of a right to privacy being encompassed within the right to personal liberty. However, it upheld regulations similar to those struck down in Kharak Singh's case, as the regulations in Gobind had a statutory foundation.

In *R. Rajagopal v. State of Tamil Nadu*[8], commonly referred to as the "Auto Shankar case", the Supreme Court held that the right to privacy, or the right to be left alone, is protected under Article 21 of the Constitution. Further it is held that every citizen has the right to safeguard the privacy of personal matters, including those related to their family, marriage, procreation, motherhood, childbearing, education, and other similar aspects. Publishing information pertaining to these matters without the individual's consent whether accurate or otherwise, and regardless of whether it is commendatory or critical constitutes a violation of their right to privacy. Such actions may render the publisher liable to legal action for damages. However, this rule is subject to exceptions. The first exception permits the publication of such matters if they are part of the public record, including court records, as these become unobjectionable. Once a matter enters the public domain, the right to privacy no longer applies, and it becomes a legitimate subject for commentary by the press, media, and others. The second exception states that public officials cannot claim the right to privacy or seek damages for criticism related to the performance of their official duties, even if the publication contains false information, unless they can prove that the statements were made with reckless disregard for the truth.

[7] AIR 1975 SC 1378.
[8] (1994) 6 SCC 632.

In *State of Maharashtra v. Madhukar Narayan Mardikar*[9], the Supreme Court held that even a woman of "easy virtue" is entitled to her right to privacy, and no one has the authority to violate it at their discretion.

In the case of *Ms. X v. Mr. Z*[10], the wife filed a petition for dissolution of marriage under Section 10 of the Divorce Act, citing cruelty and adultery by her husband. In response, the husband accused his wife of engaging in adulterous relationships. The wife had previously undergone a pregnancy termination at the All India Institute of Medical Sciences (AIIMS), where records and slides of the foetal tissue were preserved. The husband subsequently filed an application requesting a DNA test of the preserved slides to determine whether he was the biological father of the foetus. The Court ruled that while the right to privacy is a fundamental right under Article 21 of the Constitution, it is not absolute. Once information becomes part of a public record, an individual cannot claim that a DNA test would violate their right to privacy. The Court noted that the foetus, having been preserved at AIIMS, was no longer part of the wife's body, and she had already been discharged from the hospital. Thus, she could not argue that the test would infringe upon her privacy. Given that adultery was cited as a ground for divorce, the Court permitted the husband's request for a DNA test on the preserved slides.

Right to Privacy in Virginity Test: In *Surjit Singh Thind v. Kanwaljit Kaur*[11], the wife sought a decree of nullity of marriage, claiming that the marriage had never been consummated due to the husband's impotence. The husband, in his defense, asserted that the marriage had been consummated and that he was not impotent. To challenge the wife's claim of being a virgin, the husband filed an application requesting her medical examination. The Court held that subjecting a woman to a medical examination to determine her virginity would violate her right to privacy under Article 21 of the Constitution. Such an order would amount to an intrusive and degrading inquiry against a vulnerable individual. Furthermore, the Court emphasized that a virginity test cannot serve as the sole basis to establish whether a marriage has been consummated.

[9] (1991) 1 SCC 57: AIR 1991 SC 207.
[10] AIR 2002 Del 217.
[11] AIR 2003 P&H 353.

In May 2013, The "two-finger test" was held unconstitutional in the case of *Lillu @ Rakhi v. State of Haryana*[12]. In this case, the Punjab and Haryana High Court ruled that the practice of conducting the two-finger test on women to determine whether they are virgins or to check their sexual history is a violation of their fundamental rights, including the right to dignity and privacy under Article 21 of the Indian Constitution. The Court held that rape victims are entitled to legal recourse that does not cause further trauma or violate their physical or mental integrity and dignity. It emphasized that medical procedures must be conducted in a way that respects the victims' right to consent and protects their right to privacy. Further in the same year, the Supreme Court of India ruled that the two-finger test, used to assess a woman's virginity or sexual history, violates a woman's right to privacy. The Court emphasized the need for better medical procedures to confirm sexual assault. Citing international human rights standards, such as the International Covenant on Economic, Social, and Cultural Rights (1966) and the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985), the Court affirmed that rape survivors are entitled to legal recourse that does not re-traumatize them or violate their physical and mental integrity and dignity.

In April 2022, the Madras High Court directed the state to ban the two-finger test. In the same year, in the *State of Jharkhand v. Shailendra Kumar Rai*[13] case, the Supreme Court bench constituting Justices D.Y. Chandrachud and Hima Kohli, while deciding the case, reiterated the ban on the practice, ruling that a woman's sexual history is irrelevant in determining whether the elements of rape under Section 375 of the Indian Penal Code are met. The Court also stated that it is both patriarchal and sexist to disbelieve a woman's claim of rape solely because she is sexually active, reaffirming the importance of upholding the dignity and rights of women in such cases.

Telephone Tapping: In *Rayala M. Bhuvaneswari v. Nagaphamender Rayala*[14], the petitioner filed for divorce and sought to use recordings of his wife's conversations with others, made without her knowledge, as evidence. The wife denied certain portions of the conversation. The Court ruled that the husband's act of secretly recording his wife's conversations with others was illegal and violated her right to privacy under Article 21 of the Constitution. It stated that these recordings, even if true, could not be admitted as evidence. The Court also held that the

[12] (2013) 14 SCC 643.
[13] (2022) 4 SCC 259.
[14] AIR 2008 AP 98.

wife could not be compelled to undergo a voice test for comparison. The Court emphasized that the fundamental basis of marriage is trust, and the husband's actions in recording private conversations without his wife's consent clearly infringed upon her privacy. If a husband harbors such distrust, even regarding conversations with her parents, the very foundation of marriage is compromised.

In *People's Union for Civil Liberties vs. Union of India*[15], commonly known as the "Phone Tapping Case," the Supreme Court held that Section 5(2) of the Indian Telegraph Act, 1885, which authorizes the central or state government to tap telephones, constitutes a significant invasion of an individual's right to privacy. This right is an integral part of the right to life and personal liberty under Article 21 of the Constitution. The Court emphasized that telephone tapping should only be permitted in cases of public emergency or for reasons of public safety. With the advancement of sophisticated communication technologies, the right to private telephone conversations in one's home or office is increasingly vulnerable to abuse. The Court observed that, without a just and fair procedure to regulate the exercise of power under Section 5(2) of the Act, it is impossible to safeguard citizens' rights guaranteed under Articles 19(1)(a) and 21 of the Constitution. Further, in *District Registrar and Collector v. Canara Bank*[16], it was held that telephone-tapping amounts to violation of right to privacy. Hence, the right to privacy includes telephonic conversation. Therefore, telephone-tapping amounts to its violation unless it is permitted under procedure established by law.

RTP in HIV Case: In *X v. Hospital 'Z'*[17], An HIV positive individual does not have an absolute right to privacy preventing a doctor from disclosing their status, nor an unconditional right to marry under Article 21 of the Constitution. The right of others to a healthy life takes precedence, justifying a breach of confidentiality in such circumstances.

RTP in Polygraph and brain mapping tests: In *Smt. Selvi and Ors. V. State of Karnataka* (2010), the Supreme Court held that the results of polygraph and brain mapping tests could be seen as compelled evidence and would violate the constitutional protection against self-incrimination, which is violation of Article 20(3). The Court also emphasized that using polygraph (lie detector) and brain mapping tests could have a significant impact on an

[15] AIR 1997 SC 568.
[16] AIR 2005 SC 186.
[17] (1998) 8 SCC 296.

individual's mental integrity and personal autonomy, which are integral parts under Article 21. Subjecting an individual to these tests without consent was deemed an infringement on their RTP.

The concept of the right to privacy has evolved through various cases over the years, gaining its full recognition and significance in the landmark **Puttaswamy case** (2017). This judgment not only affirmed the existence of privacy as a fundamental right but also elaborated on its scope and importance in safeguarding individual autonomy and dignity.

THE RISE OF MASS SURVEILLANCE FOR NATIONAL SECURITY AND CRIME PREVENTION

Mass surveillance in India encompasses the large-scale monitoring of individuals' activities, communications, and data by government agencies. While intended for purposes such as national security, crime prevention, and public safety, mass surveillance raises significant concerns regarding privacy, civil liberties, and the potential for misuse. The legal framework governing mass surveillance in India is shaped by various statutes, regulations, and judicial interpretations.

The Indian Telegraph Act, 1885, under **Section 5(2)**, permits the government to intercept telephonic communications on grounds such as public safety, sovereignty, or national security, provided a lawful order is issued by a competent authority with a justified necessity for the action. Similarly, the Information Technology Act, 2000, through **Section 69**, authorizes the government to intercept, monitor, and decrypt information from any computer resource for reasons such as public order, national security, and crime prevention. This provision is further supplemented by the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009, which outline procedural safeguards for such surveillance.

The Unlawful Activities (Prevention) Act, 1967 (UAPA) provides the legal foundation for the surveillance of individuals suspected of engaging in unlawful activities, including terrorism and extremism, allowing for preventive detention and monitoring of suspects without prior judicial approval under certain conditions. Similarly, the National Security Act, 1980 (NSA) enables preventive detention and surveillance of individuals considered threats to national

security, public order, or essential services. Additionally, the Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, primarily designed to regulate commercial communications, intersects with surveillance by mandating the collection and storage of customer data by telecom operators, which authorities can access under specific circumstances. Together, these laws and regulations contribute to the legal framework for surveillance in India.

Furthermore, the Indian Post Office Act, 1898 allows the interception of postal articles under specific circumstances, such as maintaining public order or ensuring national security, reflecting the historical roots of surveillance mechanisms in India. Together, these statutes form the core legal framework for communication and data interception in the country.

The need for mass surveillance is often justified by governments and agencies as a tool for enhancing national security, maintaining public order, and preventing crime. Some of the key reasons often cited for the implementation of mass surveillance are:

i. National Security: Mass surveillance is often considered an essential tool for identifying and mitigating threats to national security, including terrorism, espionage, and organized crime. By monitoring communications, activities, and networks, intelligence agencies are able to detect potential risks and take preventative measures before any attack or incident occurs.
ii. Crime Prevention and Law Enforcement: Surveillance contributes to the identification and investigation of criminal activities. By collecting data on individuals and groups, law enforcement agencies can more effectively track suspects, solve crimes, and gather evidence necessary for prosecution.
iii. Public Safety: In instances of civil unrest, mass surveillance is employed to monitor public spaces and track potentially dangerous individuals or groups. It is often argued that such surveillance assists law enforcement in maintaining control during volatile situations, thereby ensuring the safety and security of the general public.
iv. Countering Cyber Threats: With the increasing sophistication of cyber crime and cyber terrorism, mass surveillance plays a critical role in monitoring internet traffic, communications, and other cyber activities to prevent attacks on vital infrastructure, businesses, and citizens.
v. Prevention of Terrorism: One of the primary justifications for mass surveillance is to identify and disrupt terrorist activities before they can be executed. Through the

monitoring of online communications, financial transactions, and physical movements, governments aim to detect and prevent the planning or coordination of terrorist acts.

Many legal systems permit exceptions to privacy rights in matters of national security. For instance, the USA PATRIOT Act, introduced following the September 11, 2001, terrorist attacks, broadened the surveillance capabilities of U.S. intelligence agencies. Similarly, the United Kingdom's Investigatory Powers Act (2016) authorizes extensive data collection and communication interception.

Government Policies and Initiatives:

Aadhaar Project: While primarily an identity system, Aadhaar involves extensive data collection, including biometric and demographic information. Access to Aadhaar data by various government agencies for service delivery has implications for surveillance and privacy.

Central Monitoring System: Established by the Department of Telecommunications, CMS is intended to monitor all telecommunications in real-time to aid in national security and law enforcement. Its implementation has raised concerns about mass data collection without adequate oversight.

Surveillance and Monitoring of Public Spaces: Deployment of Closed-Circuit Television (CCTV) cameras across cities under initiatives like "Smart Cities Mission" facilitates real-time monitoring of public spaces, contributing to mass surveillance capabilities.

RIGHT TO PRIVACY AND MASS SURVEILLANCE - AN INTERNATIONAL PERSPECTIVE

Mass surveillance refers to the extensive collection and analysis of data, often without targeting specific individuals. It involves the use of technologies such as facial recognition, data mining, phone tapping, and internet monitoring to track citizens and identify potential threats. The growing reliance on surveillance technologies has been largely driven by global security concerns, particularly following events like the September 11, 2001, terrorist attacks.

Two prominent examples of mass surveillance legislation are the USA PATRIOT Act and the UK's Investigatory Powers Act. Enacted after the 9/11 attacks, the USA PATRIOT Act expanded the surveillance powers of U.S. intelligence agencies, allowing them to monitor

individuals, including foreign nationals, both domestically and internationally. Similarly, the UK's Investigatory Powers Act (2016), also known as the "Snooper's Charter," grants the government broad authority to collect and store communication data. This section examines these legal frameworks, the extent of their surveillance capabilities, and the justifications provided by governments for implementing such measures.

RTP under the International Frameworks:

The right to privacy is a fundamental human right recognized in international and regional legal instruments. The Universal Declaration of Human Rights (UDHR), 1948, under **Article 12**, protects the individuals against arbitrary interference with privacy, family, home, or correspondence and guarantees the right to legal protection against such intrusions.

Similarly, the International Covenant on Civil and Political Rights (ICCPR), 1966, under **Article 17**, explicitly recognizes the right to privacy, mandating that states ensure any limitations on this right are lawful, necessary, and proportionate. In addition, **Article 19** of both the UDHR and ICCPR upholds the right to freedom of expression and the right to hold opinions without interference, which may be threatened by mass surveillance practices that promote self-censorship.

Regional human rights instruments also reinforce these principles: the European Convention on Human Rights (ECHR), 1950, guarantees the right to respect for private and family life under **Article 8**, subject to lawful and necessary limitations in a democratic society; the American Convention on Human Rights (ACHR), 1969, protects privacy and personal honor under **Article 11**; and the African Charter on Human and Peoples' Rights, 1981, while not explicitly recognizing privacy, emphasizes the right to dignity and freedom, indirectly supporting privacy protections. Together, these provisions form a robust framework for safeguarding privacy and related rights globally.

The UN High Commissioner for Human Rights has consistently highlighted concerns regarding mass surveillance, stating that arbitrary or unlawful surveillance violates the right to privacy and freedom of expression.

Cases relating to the RTP by the European Court of Human Rights:

In *Big Brother Watch v. United Kingdom (2021)*, the European Court of Human Rights

emphasized the need for independent oversight of bulk interception practices and proper safeguards to ensure compliance with Article 8.

The case *Liberty and Others v. the United Kingdom (2008)* involved the UK Ministry of Defence intercepting the communications of civil liberties organizations under a broad warrant issued with wide discretionary powers. The European Court of Human Rights ruled that this violated the organizations' right to privacy under Article 8 of the European Convention on Human Rights. The Court found that the UK's legal framework for intercepting communications lacked sufficient safeguards and oversight, allowing for excessive and unchecked surveillance. As a result, the Court determined that the interception was disproportionate and violated the right to privacy.[18]

Similarly, in the case *Roman Zakharov v. Russia (2015)*, the European Court of Human Rights found that Russia's system for covert interception of communications violated the right to privacy under Article 8 of the European Convention on Human Rights. The Court ruled that the system lacked adequate safeguards, gave authorities excessive discretionary powers, and provided no effective remedies for individuals to challenge surveillance or seek redress. This created a high risk of arbitrary interference with privacy, leading to a violation of fundamental rights.[19]

However, the International law does not prohibit surveillance outright but requires a careful balance between state interests and individual rights. The principles of legality, necessity, and proportionality serve as a guide to ensuring that surveillance measures respect fundamental freedoms. Additionally, transparency and independent oversight are critical for holding governments accountable and maintaining public trust.

STRIKING A BALANCE BETWEEN THE RIGHT TO PRIVACY AND MASS SURVEILLANCE

The Justice K.S. Puttaswamy (Retd.) and Anr. V. Union of India and Ors. (2017)[20] case is a landmark judgment by the Supreme Court of India that recognized the right to privacy as a fundamental right under the Indian Constitution. This case arose when Justice K.S.

[18] https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e.
[19] ibid
[20] (2017) 10 SCC 1.

Puttaswamy, a retired High Court judge, and others challenged the constitutional validity of the Aadhaar Card Scheme of the Government of India, arguing that it violated individuals' privacy rights. Aadhaar, a biometric-based unique identification system, was being increasingly used for public services, raising significant concerns about surveillance, data security, and potential misuse of personal information. The core constitutional questions revolved around whether the right to privacy was a fundamental right and whether the Aadhaar scheme infringed upon it by collecting and storing personal data. The petitioners argued that privacy is implicitly protected under Part III of the Constitution, particularly Articles 14 (Right to Equality), 19 (Right to Freedom), and 21 (Right to Life and Personal Liberty), emphasizing the risks of mass surveillance and data breaches. On the other hand, the Union of India contended that privacy was not explicitly mentioned as a fundamental right in the Constitution and that Aadhaar served legitimate state interests such as preventing fraud and ensuring efficient delivery of subsidies.

On August 24, 2017, a nine-judge Constitution Bench delivered a unanimous verdict, declaring that the right to privacy is intrinsic to life and liberty and is protected under Article 21, with connections to other fundamental rights like freedom of speech and equality. The Court overruled earlier judgments in M.P. Sharma (1954) and Kharak Singh (1962) that had denied privacy as a fundamental right. However, the Court clarified that privacy is not absolute and can be subject to reasonable restrictions, provided any intrusion satisfies the tests of legality, necessity, and proportionality. While the judgment did not directly address the Aadhaar scheme's validity, it laid the foundation for later cases to scrutinize it. This ruling is a constitutional landmark, reaffirming the dynamic and evolving interpretation of fundamental rights and strengthening civil liberties by protecting individual autonomy, dignity, and personal data in the digital age. It also influenced subsequent rulings on Aadhaar and catalyzed the development of data protection policies in India. In a related 2018 case, the Supreme Court upheld the Aadhaar Act's constitutionality with restrictions, balancing privacy concerns with state interests. The Puttaswamy judgment remains a foundational precedent for legal and policy discussions surrounding privacy, surveillance, and digital rights in India.

Striking a balance between the RTP and Mass Surveillance is a complex challenge, especially in an age of technological advancements. While mass surveillance can be crucial for national security, law enforcement, and crime prevention, it must not infringe upon individuals' fundamental right to privacy. This balance requires a legal framework that ensures surveillance

is conducted lawfully, with clear standards of necessity, proportionality, and non-arbitrariness. Effective oversight mechanisms are essential to prevent abuse, ensuring transparency and accountability. Surveillance practices should be subject to judicial review, and individuals should be informed about the extent of data collection and monitoring. Technological safeguards, such as data protection, anonymization, and secure storage, are crucial to minimize risks of misuse. Moreover, surveillance should be proportional to the threat it seeks to address, with data minimized and retained only as long as necessary. International human rights standards emphasize that any interference with privacy must be lawful, necessary, and proportionate. In conclusion, maintaining this balance requires careful regulation, oversight, and respect for privacy rights while addressing legitimate security concerns.

Post the Puttaswamy judgment, any surveillance measures must comply with the principles of legality, necessity, and proportionality. Courts have the authority to review and strike down surveillance practices that violate fundamental rights. The legal expectations now include incorporating privacy considerations into the design and implementation of surveillance technologies and policies to mitigate undue intrusions.

THE FUTURE OF DATA PROTECTION

The enactment of laws such as the UK's Investigatory Powers Act, 2016 and the global rise in digital surveillance technologies influenced India to strengthen its domestic surveillance capabilities. The government's efforts to expand surveillance for national security reasons, alongside ongoing debates about privacy, spurred calls for more robust data protection laws. This culminated in the drafting of the Personal Data Protection Bill and a growing focus on scrutinizing surveillance practices.

The Personal Data Protection Bill (PDP Bill) is proposed legislation in India aimed at safeguarding individuals' personal data and creating a comprehensive framework for data privacy. It defines personal data as any information that can identify an individual, such as names, contact details, and biometric data. The bill distinguishes between "data fiduciaries," which are entities that collect and process data, and "data principals," the individuals whose data is processed, outlining the responsibilities of data fiduciaries to ensure that data is handled fairly and securely. The key provisions include the requirement for explicit consent from individuals for data collection, the right of individuals to access, correct, erase, and port their

data, and the establishment of a Data Protection Authority to oversee compliance. The bill also mandates data localization for certain sensitive data, requiring it to be stored within India, and introduces stringent penalties for non-compliance. Additionally, it addresses cross-border data transfers and mandates breach notifications to affected individuals. While the bill aligns with global privacy standards like the EU's General Data Protection Regulation (GDPR), 2018, it has faced criticism regarding provisions for state access to data and data localization requirements. Nevertheless, the PDP Bill represents a significant step toward strengthening data privacy in India, ensuring greater protection and accountability in the digital landscape.

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark legislation enacted by the Indian government to establish a robust framework for safeguarding digital personal data. It applies to data processing within India and to entities outside India if they offer goods or services to individuals in the country. The Act outlines the rights of individuals (referred to as Data Principals), including the right to access, correct, and erase personal data, and provides mechanisms for grievance redressal and data-related nominations. On the other side, it imposes strict obligations on entities processing this data (Data Fiduciaries), such as obtaining valid consent, conducting data protection impact assessments, implementing security safeguards, and notifying breaches. A key feature of the Act is the establishment of the Data Protection Board of India (DPBI), an independent adjudicatory body responsible for ensuring compliance and imposing penalties that can reach up to ₹250 crore for major violations, especially concerning children's data and security breaches. The Act allows cross-border data transfers except to countries restricted by the government, with special provisions for the protection of children's data, requiring parental consent for those under 18 and banning targeted advertising. Compared to the EU's GDPR, the DPDP Act focuses solely on digital data and does not differentiate between categories of data, though it mirrors GDPR's extraterritorial scope. Certain exemptions are provided for legal, judicial, and law enforcement purposes. Implementation is being rolled out in phases, with the government in the process of establishing operational rules and the Data Protection Board. Overall, the DPDP Act represents a significant advancement in India's digital governance, aligning with global privacy standards while catering to the country's specific regulatory needs.

SUGGESTIONS

Balancing the RTP with mass surveillance requires careful consideration of security needs and individual freedoms. The following are the suggestions:

i. Establishing clear legal boundaries by defining the scope and limits of surveillance in transparent legislation and clearly specify which agencies have surveillance powers, under what conditions, and for what purposes.
ii. The current act such as the **Information Technology Act, 2000** could be revised to include robust provisions for safeguarding personal data rather than introducing a completely new framework through the Personal Data Protection Bill.
iii. Creating the independent oversight bodies to monitor surveillance programs and ensure compliance with privacy laws, in addition to conduct periodic reviews of surveillance activities to assess their effectiveness and necessity.
iv. Requiring judicial authorization i.e., the court approval for intrusive surveillance measures. Implement a system of checks and balances to ensure judicial decisions are informed and impartial.
v. Limiting the collection of data to what is strictly necessary for specific security purposes.
vi. Improving transparency and public accountability by publishing regular reports on surveillance activities, including the number of requests made and approved.
vii. Ensure that surveillance measures adhere to the principles of proportionality and necessity, being commensurate with the level of threat and essential for achieving clearly defined security objectives.
viii. Using encryption and secure storage methods to protect collected data from unauthorized access.
ix. Educate the public about their privacy rights and the extent of surveillance practices. Engage civil society and privacy advocacy groups in policy making to represent diverse perspectives.
x. Implementing strict penalties for individuals or agencies that misuse surveillance powers. Establish mechanisms for citizens to challenge unlawful surveillance and seek redress.

CONCLUSION

The landmark Puttaswamy's case plays a vital role in shaping and significantly strengthened the right to privacy in India by affirming it as a fundamental right under Article 21 of the Constitution. This judgment recognized privacy as essential to life, liberty, and dignity,

protecting individuals from arbitrary state actions. It impacted key areas such as the Aadhaar system, highlighting the need for safeguards against the misuse of personal data and driving the call for data protection legislation like the Personal Data Protection Bill. The ruling also addressed digital privacy concerns, empowering individuals against unauthorized surveillance and data collection. It further safeguarded marginalized groups by protecting sensitive information, such as sexual orientation and health status, from discrimination. By reinforcing civil liberties and supporting personal autonomy, the judgment aligned India with international human rights standards and set a precedent for future legal reforms, including regulations on surveillance and data security. The Puttaswamy case has, therefore, been a catalyst for redefining privacy in India, ensuring its protection in an increasingly digital world.

In conclusion, striking a balance between the right to privacy and the requirements of mass surveillance is a challenging yet essential aspect of modern governance. While surveillance is critical for national security and crime prevention, it must not undermine fundamental human rights. Establishing clear legal frameworks, implementing strong oversight mechanisms and adhering to the principles of proportionality and necessity are crucial for achieving this balance. By promoting accountability, limiting data collection, and utilizing privacy-preserving technologies, governments can safeguard both their citizens and their privacy. Maintaining this balance necessitates ongoing dialogue, active public involvement, and a steadfast commitment to democratic principles in an increasingly interconnected world.

REFERENCE

Universal Declaration of Human Rights (UDHR)
International Covenant on Civil and Political Rights (ICCPR)
Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)
State of Jharkhand v. Shailendra Kumar Rai (2022)

BOOKS:

Constitution of India by V. N. Shukla, 13th Edition.
Constitutional Law of India by Dr. J.N. Pandey, 52nd Edition.
Constitutional Law of India by Dr. J. N. Pandey, 58th Edition.
The Constitution of India by B M Bakshi, 15th Edition.

ONLINE SOURCES:

Venkatesh Nayak, Slide 1, (Oct. 13, 2012), https://cic.gov.in/sites/default/files/2012/R2Privacy-Venkatesh.pdf.

Oishika Banerji, Different aspects of Right to Privacy under Article 21 - iPleaders, IPleaders (Dec. 6, 2021), https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/.

Right to Privacy, (Oct. 21, 2022), https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-privacy-3.

Thin Safeguards and Mass Surveillance in India, https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1188&context=nlsir.

https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e.

Lysanne Louter, Mass Surveillance, Security and Human Rights, Amnesty International Canada https://amnesty.ca/what-we-do/surveillance-security-and-human-rights/.