ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

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

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, 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

ISSN: 2582-6433

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 8Articles in various reputed Law Journals. Conducted 1Moot 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-1, 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.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS 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.

www.ijlra.com
Volume 2 Issue 7 | June 2023
ISSN: 2582-6433

SURVEILLANCE VIS-À-VIS RIGHT TO PRIVACY IN INDIA

AUTHORED BY - RAHUL RAMCHANDRAN

ABSTRACT

The act of surveillance involves observing or monitoring individuals, groups, or organizations and can be conducted by governments, private entities, or individuals. The reasons for surveillance may vary, such as for national security, law enforcement, or corporate espionage. However, this practice can sometimes lead to the violation of one's right to privacy. The Constitution of India safeguards the right to privacy in Article 21, which asserts that no individual can be stripped of their personal liberty or life unless done so through the proper legal procedures. This provision serves as a cornerstone of the Indian legal system, ensuring that citizens are protected from unwarranted intrusions into their private lives. The use of technology for surveillance purposes has brought about much debate in recent years in India. The government has implemented various surveillance measures, including CCTV cameras in public places and electronic communication interception, in the name of maintaining law and order and national security. However, such measures have been criticized for infringing upon citizens' right to privacy. In 2017, the Indian Supreme Court ruled that privacy is a fundamental right and any interference with it must be justified by a compelling state interest and must be proportionate. Additionally, the government has been criticized for a lack of transparency and accountability in its surveillance activities. It is necessary to establish a strong legal framework to regulate surveillance activities in India and proper oversight mechanisms to ensure that such activities abide by the law and do not violate citizens' right to privacy.

Keywords: Surveillance, Right to Privacy, Article 21, Technology, Violation

ISSN: 2582-6433

TABLE OF CONTENT

ISSN: 2582-6433

- **BACKGROUND:**

In the digital era, the debate over monitoring and the right to privacy has taken on more importance. Concerns regarding the preservation of personal privacy have been raised as a result of the development of technology and the widespread use of digital communication platforms, which have made it possible for both public and private entities to engage in various types of monitoring. A fundamental human right, the right to privacy is one that is recognised by several international and state law systems. It covers the freedom from unjustified interference with one's private life, which includes private communications, actions, and data. However, the conventional definitions of privacy have been put to the test by the development of surveillance technology.

- **RESEARCH PROBLEM**

Surveillance has the potential to infringe upon an individual's right to privacy by gathering their personal information without their permission, monitoring their whereabouts, and observing their online behaviour. It can also be utilized to restrict and suppress freedom of speech or influence public sentiment. Additionally, it opens the door to prejudicial treatment and the possibility of those in power abusing their authority.

- **LITERATURE REVIEW**

1). Anubhav Khamroi and Anujay Shrivastava, Scrutinizing the Applied Implications of a Right to Privacy: State Surveillance And Constitution, 2019.

The paper examined several cases where the right to privacy and state surveillance have come into conflict, including the Aadhaar card scheme and the use of surveillance technologies like CCTV cameras and facial recognition. The authors argued that there needs to be a balance between the right to privacy and the needs of the state and that the Constitution provides for this balance through its restrictions on the right to privacy. It also discussed the role of the judiciary in protecting the right to privacy and ensuring that state surveillance is carried out in a manner that is consistent with the Constitution. The authors noted that the use of technology has made it easier for the state to carry out surveillance and call for greater regulation of this use to ensure that it is consistent with the right to

ISSN: 2582-6433

privacy. The paper concluded by arguing that the right to privacy is an essential right that must be protected as well as balanced against the needs of the state.

2). Dr. G. Mallikarjun and B. Md. Irfan, Right to Privacy in India: The Technical And Legal Framework, 2022.

This article states that the largest drawback of Article 21's right to privacy is that both the text and its legal interpretation are inherently in disagreement with how privacy issues are typically discussed. It further adds that in today's society, privacy continues to be portrayed as a private, communal, or human right that states must defend, unless there are serious threats to national security. It continues with the fact that the right to privacy vs security dilemma can be such a type that governments often get away with compromising the privacy of their citizens under the guise of "national interest".

3). Sangeeta Mahapatra, Digital Surveillance and the Threat to Civil Liberties in India, 03 May 2021.

The paper discussed how digital surveillance technologies, such as CCTV cameras, social media monitoring, and facial recognition, have become pervasive in India and can potentially infringe upon individual privacy rights. The author examined the current legal framework for surveillance in India and the role of the judiciary in protecting civil liberties. The author also discussed how surveillance can be used to stifle dissent and undermine democratic values. The paper concluded by calling for greater public awareness about the potential impact of digital surveillance on civil liberties and the need for greater accountability and transparency in the use of these technologies by the state.

4). ***The State of Surveillance in India: The Central Monitoring System's Chilling E s Chilling Effect on Self-Expr ect on Self-Expression by Addison Litton, 2015.***

In the interest of expounding upon the ongoing dialogue surrounding governmental surveillance, particularly in the Indian realm, this writing endeavors to posit an argument concerning the Central Surveillance Systems (or better known as "CMS"), which at its core, poses an unmistakable and impending danger to both privacy and the democratic tenets of free expression. With this in mind, this exposé aims to detail how this very CMS could potentially usher in an entirely new era with respect to regulating language within the Indian borders, shifting away from the status quo of "private

ISSN: 2582-6433

censorship" and towards an alarming increase in self-censorship among the nation's telecommunications providers, thus leading to widespread suppression of civilian speech under the pernicious regime of the CMS.

5). ***Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles - By Maria Xynou, 2015.***

In the opus at hand, the writer posits that the Indian government - by means of its sundry regulations and service provider licensing agreements - has put in place a legal architecture which buttresses the authorities in executing surveillance endeavours. The Center for Internet and Society (CIS) concedes that surveillance, when executed lawfully, legitimately and in a targeted manner can be a salutary weapon in advancing the cause of law enforcement, particularly in the battle against criminality and terrorism. However, in certain cases, existing laws and licensing agreements in India manifestly put a strain on the capacity of the government to engage in surveillance, while yoking up individuals' rights to enjoy confidentiality and to have their data protected.

6). ***The Digital Person: Technology and Privacy in the Information Age Daniel J. Solove, October 1, 2004***

It is beyond dispute that the advancements in technology have indubitably shifted our perception of privacy. The antiquated notions we had are no longer efficacious in dealing with the exigencies brought on by the rapid digitalization of the world. The legal framework that governs our privacy is couched in these outmoded concepts and has proven it impotent in the face of the surging privacy concerns stemming from digital dossiers. However, this book seeks to upend the established paradigms of our understanding of privacy and reimagines the very foundation of privacy to cope with the unprecedented challenges of our existence in the unprecedented Information Age.

7). Privacy, free expression and transparency Redefining their new boundaries in the digital ageJoseph Mifsud BonniciEvgeni Moyakine, 2016

The study examines and decodes several complex issues. In particular, this study examines the complex relationship between the right to freedom of expression (including the right to access information), transparency, and Internet privacy. The study examines the limits of these rights and

ISSN: 2582-6433

explores different ways of harmonizing and unifying them. The study analyses the legal framework, current legal settlement mechanisms as well as specific issues, cases and trends. As research has shown, standard laws and regulations to protect privacy and free speech often rely on addressing digital issues. Furthermore, the study covers interactions between multiple stakeholders, including government agencies, ICT companies, Internet users, civil society organizations, the judiciary, and security services. The study recommends different policies to address key issues and different stakeholders.

8). ***Alan F. Westin, Privacy And Freedom, March, 1967.***

Ellen Westin's "Privacy and Freedom" provides a detailed and comprehensive analysis of the conflict between privacy and surveillance in modern society. Prepared under the auspices of the Special Committee on Science and Law of the New York City Bar Association, with funding from the Carnegie Corporation, this book will undoubtedly be considered an essential reference on this topic. The book is divided into four parts: (1) the role of privacy in society; (2) a description of technological advances in surveillance; (3) the response of American society to the introduction of these new technologies; (4) an assessment of the past of American law in this area. and future effects. In the first of these sections, the authors introduce the social value of privacy, an approach conspicuously lacking in other surveillance works.

9). ***A Typology of Privacy by BERT-JAAP KOOPS, June, 2017***

According to the authors by utilizing a two-dimensional model, we are able to categorize various types of privacy into eight distinct categories, including bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioural privacy. This model also includes a ninth category, informational privacy, which intersects with the other eight but is not identical to them. The scope and comprehensiveness of this analysis make it a significant contribution to the theoretical literature on privacy. Our typology is a valuable tool for analysing and understanding the nature of privacy, its relationship to the right to privacy, and how this right varies and corresponds across different countries. It is important to note that privacy cannot be reduced to informational privacy alone.

ISSN: 2582-6433

10). ***The "Criminal Tribe" and Independence: Partition, Decolonisation, and the State in India's Punjab, 1910s-1980s Sarah Eleanor Gandee, August, 2018.***

The author in the article has contended that with no central watchdog, tribal surveillance is part of day-to-day police management. The system had an inevitable flaw in that while there were severe penalties for breaking the law, there were few opportunities for reform for those tribe members who were genuinely interested in living an honest life.

- **SCOPE AND OBJECTIVES**

This research paper aims to analyse the history and origin of privacy in India. This research paper includes the importance of surveillance in India. It discusses the statues and laws applicable to surveillance in India. It also talks about the infamous Puttaswamy judgment with regards to right to privacy. This paper also covers various cases where the Courts have pressed on the importance of such a right. It looks into how surveillance is affecting the right to privacy of the people in India.

- **METHODOLOGY**

The research has doctrinal method of research, relevant reference from various literature, committee reports, precedents, journals & books are cited.

- **RESEARCH QUESTIONS**

What are the laws governing surveillance in India, and how far has such surveillance had a negative effect on the right to privacy?

- **HYPOTHESIS**

Right to Privacy is not protected in India due to Surveillance.

ISSN: 2582-6433

CHAPTER II: CONCEPT OF SURVEILLANCE

- **SURVEILLANCE AND INDIAN LAW REGIME**

Surveillance refers to the act of a third-party monitoring, collecting, or intercepting an individual's data. With the rise in technology and the increasing number of people using telecommunication and the internet in India, there is a greater likelihood that personal and confidential data can be shared through these means without knowledge of a third-party interceptor. To prevent this, India has implemented legislation to regulate the surveillance of calls and websites. While strict surveillance can be useful in monitoring national security and criminal activity, only certain authorized departments and individuals are permitted to monitor and intercept data, and their reasons must align with the clauses outlined in the legislation. The right to privacy is a fundamental human right, and the Indian Constitution recognizes and upholds this principle for all its citizens. By safeguarding the right to privacy, the Indian legal system ensures that individuals can live their lives free from unnecessary interference and intrusion. This protection is crucial for maintaining the dignity and autonomy of citizens and upholding the values of democracy and justice.

The profound author David Lyon has expressed his belief in the intricate world of surveillance, positing that it encompasses the relentless monitoring of individuals' behaviours, activities, and other dynamic and mutable information, all for the purpose of furthering a given objective, whether it be exerting influence, managing scenarios, directing actions, or safeguarding individuals' safety and security. The Indian Constitution, which is imbued with a profound and ennobling sense of purpose, invests the Parliament with the authority to promulgate laws concerning surveillance while also ensuring that the fundamental rights of individuals are scrupulously upheld and protected.

India, a nation of diverse and multifarious people and beliefs, has promulgated manifold laws on the subject of surveillance. According to the wise and insightful words of David Lyon, the usage of surveillance entails the meticulous observation of the behaviour, activities, or other constantly shifting data of individuals in order to influence, manage, direct, or even safeguard them.[1] As such, the implementation of surveillance by the government enables the authorities to sustain and protect the

[1] Rabindra Kumar Mohanty. (2011). David Lyon, Surveillance Studies: An Overview, Polity: Cambridge, 2007; 256 pp.: ISBN 9780745635910, £55.00 (hbk), ISBN 9780745635927, £14.99 (pbk). International Sociology, 26(2), 284–284. https://doi.org/10.1177/02685809110260022003

ISSN: 2582-6433

lives, as well as the liberties of the people. It is within the holy grail of the Indian Constitution that the Parliament is bestowed with the power to construct laws pertaining to surveillance and its associated matters while concurrently ensuring that the fundamental rights of the individuals are safeguarded and upheld.

Throughout the annals of history, the autocratic authoritarians have been notorious for employing various forms of surveillance to quell their animus, and to oppress and reprimand their political adversaries, dissidents[2]. Under British colonialism, individuals of certain denominations were deemed perilous and perceived as inherently criminal due to their birth, beliefs and castes, thereby rendering the tribes to which they belonged as criminal syndicates. In the quest to regulate and monitor the behaviour of this marginalized segment, the British colonisers passed the Criminal Tribes Act in 1871, whereby 150 castes were designated as "hereditary criminals" and subjected to policing scrutiny.[3] The purview of this list was comprehensive, encapsulating any individual who was suspected of vocalizing their dissent against the British regime. Under the statute of 1871, the law enforcement agencies possessed boundless discretionary powers to apprehend anyone at their whim and desire, all in the name of maintaining law and order in the society. The suspects' names, fingerprints, and other personal details were meticulously recorded to enable the authorities to vigilantly monitor their every move. If the current welfare state happens to misappropriate the methods of surveillance to satiate their own ulterior political motives, thereby targeting and persecuting political dissenters, it would not be remiss to aver that such professed "welfare governments" bear a striking resemblance to their totalitarian and authoritarian counterparts.[4]

[2] A TYPOLOGY OF PRIVACY BERT-JAAP KOOPS, BRYCE CLAYTON NEWELL, TJERK TIMAN, IVAN ŠKORVÁNEK, TOMISLAV CHOKREVSKI, AND MAŠA GALIČ, Published by Penn Law: Legal Scholarship Repository, 2017, https://scholarship.law.upenn.edu/jil/vol38/iss2/4

[3] The “Criminal Tribe” and Independence: Partition, Decolonisation, and the State in India's Punjab, 1910s-1980s Sarah Eleanor Gandee, The University of Leeds and Sarah Eleanor Gandee August 2018 https://etheses.whiterose.ac.uk/22408/1/Gandee_SE_History_PhD_2018.pdf

[4] Privacy, free expression and transparency Redefining their new boundaries in the digital ageJoseph Mifsud BonniciEvgeni Moyakine Published in 2016 by the UNESCO 2016ISBN 978-92-3-100188-8, http://creativecommons.org/licenses/by-sa/3.0/igo

ISSN: 2582-6433

CHAPTER III: THE IMPORTANCE OF PRIVACY

Privacy is an essential facet of human existence because it fulfils both external and internal aspects of an individual's being. It safeguards the freedom of speech and opinion, as well as the right to hold any ideas, express dissent, associate with others, and remain anonymous. Additionally, privacy safeguards the self-determination of individuals regarding their personal choices, including decisions related to marriage, parenthood, childlessness, and sexual orientation. Alan F. Westin posits that privacy serves four functions in democratic societies: personal autonomy, emotional liberation, self-assessment, and limited and protected communication. Westin defines privacy as the right of individuals, groups, or institutions to regulate the sharing of information about themselves with others, including when, how, and to what extent. However, privacy also has implications for society, which may inhibit certain individual behaviours that are conducive to societal well-being.

Solove argued that privacy serves to enrich social interaction in numerous ways. The absence of privacy, he claims, would result in a suffocating society. When Privacy is not upheld, the consequences of improper observation on human behaviour are catastrophic and far-reaching. Overwhelming surveillance can even have severe psychological repercussions.[5]

- **LEGAL PROTECTION OF PRIVACY RIGHTS IN INDIA**

The central or state governments, along with authorized officials, have been granted the power to intercept communications in India by the Telegraph Act of 1885. This authority has been given to ensure the preservation of India's sovereignty and integrity, national security, friendly relations with foreign countries, public order, or to prevent incitement to commit a crime. The power to intercept communications, however, is not without limitations. The Indian Telegraph Rules of 1951, Section 419A specifically, provides procedural safeguards against telephone tapping.

The Information Technology Act 2000 grants law enforcement authorities the power to intercept computer communication in cases where it is deemed necessary for the integrity of India's sovereignty, national security, friendly foreign relations, public order, or in situations that may incite

[5] Privacy: practical controversies, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 83–222 (Beate Roessler & Dorota Mokrosinska eds., 2015). https://doi.org/10.1017/CBO9781107280557

ISSN: 2582-6433

a preventable and identifiable crime. The agencies hold the authority to force intermediaries or any individual to comply with their requests for such intentions.

The responsibility of overseeing computer resources to aid in message decryption lies with designated personnel. Nonetheless, the Information Technology Act is not comprehensive in its coverage. While it safeguards personal data stored electronically to a limited extent, there are no provisions in place to protect the data which may be in possession of private entities. This lack of regulations extends to all forms of personal data.

The highest authority that oversees the legal system in India is the Constitution of India. This document outlines the basic principles that regulate the country's political structure, along with the privileges and obligations of its inhabitants. It was formally accepted on November 26, 1949, and put into operation on January 26, 1950. Moreover, it is the lengthiest written constitution worldwide, with a total of 448 articles and 12 schedules included in its contents.

These principles include the preservation of individual liberties, the protection of fundamental human rights, and the promotion of social justice. When exercising its powers, the State must ensure that it is not violating the Constitution or infringing on the rights of its citizens. It is the responsibility of the State to uphold the Constitution and act in the best interests of its people.[6]

[6] A Comprehensive Note On INDIAN CONSTITUTION- A source code to billion dreams, https://loksabhadocs.nic.in/Refinput/Research_notes/English/04122019_153433_1021204140.pdf

ISSN: 2582-6433

CHAPTER III: INDIAN CONSTITUTION ON SURVEILLANCE AND PRIVACY

- **INDIAN CONSTITUTION AND SURVEILLANCE:**

The Preamble of the Indian Constitution refers to any form of limitation that impedes an individual's autonomy and independence. Securing the dignity of every individual and ensuring justice, liberty, and equality of status are undeniably integral aspects of any functional society. It is possible to ensure that every individual has equal access to opportunities in India. This is why the Indian Constitution outlines the importance of providing equal opportunities to all its citizens. By granting people the freedom to think, speak, and act as they choose, it becomes possible to guarantee that everyone has the same chances in life. This includes the right to express oneself without fear of retribution, and to pursue one's goals and dreams without discrimination. By securing these fundamental rights, India can create a society that is fair, just, and equitable for all its citizens. The Preamble acknowledges the personal autonomy and self-respect of individuals in matters of belief, faith, and worship.[7] The fundamental rights enshrined in Articles 14 (Equality), 19 (Freedom), and 21 (Right to Life) constitute the pillars of a just and fair society. The Indian Constitution's Article on Personal Liberty serves as a safeguard for protecting the basic rights and freedoms of individuals. The Honourable Supreme Court of India has consistently upheld the idea that administrative authorities must adhere to the concept of "fairness" in all their actions. This includes utilizing principles of review to evaluate discretionary and arbitrary powers.

The protection of an individual’s right allowing an individual to develop their inner and outer selves. The Indian judiciary, acknowledging the sanctity of Human Rights, has taken a liberal stance in interpreting this concept. As such, the fundamental right to privacy has been included within the scope of personal liberty.

In Kharak Singh v UP State[8], applicant was allegedly harassed by night-time police home visits. The Apex Court ruled that the home visits violated the right to life and personal liberty enshrined in Article

[7] WRIT PETITION (CIVIL) NO 494/2012
[8] Kharak Singh v UP State, (1964) 1 SCR 332

ISSN: 2582-6433

21 of the Constitution. In another case, Govind v. Congressman,[9] Mathew, J., further enacted the privacy law. In this case, it's also about home visits. The Supreme Court held that claims of privacy protections should be carefully considered and should be rejected only when there is evidence of a significant conflict of interest. If a court finds that a recognized right is entitled to protection as a fundamental right to privacy, laws violating that right must satisfy the paramount test of the national interest. The honourable Supreme Court of India rules again in Malak Singh v State of Punjab[10] case, while surveillance, Police should not be dealing with so-called bad characters, repeat offenders and would-be offender's violation of citizens' privacy. Indian judiciary considers phone hacking a serious breach of privacy.

A case addressing privacy concerns is K.S. Puttaswamy v Union of India[11], Its landmark Supreme Court decision stated, the right to privacy is at the core of the fundamental rights guaranteed by Articles 14, 15, and 21 of the Constitution. Everyone in society, regardless of social class or economic status, enjoys the autonomy to protect privacy right. Privacy as a fundamental and central feature of life and personal freedom enables individuals to stand up. Therefore, under section 5(2) of the Telegraph Act, 1885 telephone tapping would violate an individual's right to privacy unless permitted by due process under the law. To this end, courts have established certain guidelines to regulate government wiretapping.

In Selvi v State of Karnataka[12], the Supreme Court held that the compulsory use of any technique, such as anaesthesia analysis, polygraph examination and BEAP (Brain Electrical Activation Profile) testing, constituted an undue Recognize that forcible intrusion into a person's mental processes is also an attack on human dignity and freedom, often with serious and long-term consequences.

The resplendent and eminent Supreme Court of India, in its esteemed wisdom, has rendered a profound judgement deeming that Section 66A of the Information Technology Act, which addresses online offensive speech, is unconstitutional, as it endows law enforcement agencies with copious

[9] Govind v. Congressman, 1975 SCR (3) 946
[10] Malak Singh v State of Punjab, MANU/SC/0157/1980
[11] K.S. Puttaswamy v Union of India, W.P (Civil) No. 494/2012
[12] Selvi v State of Karnataka MANU/SC/0325/2010

ISSN: 2582-6433

quantities of unlimited power to thwart offensive online speech. The sacrosanct year of 2015 saw a spirited debate ensue with the Indian government arguing in favour of the concept that the right to privacy was not an intrinsic aspect of India's fundamental right to life and personal liberty, as judgments recognizing India's fundamental right to privacy were made by mere lower courts and not by the revered and elevated higher courts. The infallible Supreme Court of India, having been gravely perturbed by this confounding issue, ordered the privacy issue to be referred to a larger court as the topic was one of pressing national importance. The government, in response, conveyed with great urgency that the former judgments denying fundamental privacy rights were handed down by eight and seven judges, respectively. The court took a precautionary measure by also mandating the issuance of Aadhar cards, which served to provide a unique identification number that was not legally required. It is with great anticipation that the entire case is presently before the Supreme Court awaiting their esteemed verdict. However, it is important to note that despite the Indian Constitution empowering the Center to formulate privacy and data protection laws in the course of constitutional acknowledgment of the right to privacy, the jurisdiction is specifically conferred under Section 246(1) of the Indian Constitution. To this effect, Parliament has the power to legislate on matters listed in Schedule I of the Seventh Schedule to the Constitution. Despite list I being devoid of any entries on data protection laws or data protection laws, entry 97 provides Parliament with the power to legislate on any matter not included in List II (National List) of Schedule 7.

In the grand scheme of legal jargon, nestled unassumingly within Schedule III of Schedule 7 (the Concurrent Schedules), lurks Entry 97, a clause resplendent with profound potential. You see, absent any explicit data protection provisions gracing the other catalogues, this particular entry furnishes Parliament with residual capabilities to bestow legal clout upon virtually any matter of national purport, even - dare I say it - the hallowed 'right to privacy' and the captivating domain of data protection..[13] In the contemporary interconnected world, India finds itself subject to intercontinental scrutiny and foreign pressure to effectively and securely legislate data privacy laws. In accordance with Article 253 of the Indian Constitution, parliamentary authorities are granted the power to pass legislation essential to further the implementation of any international agreement or accord. Despite the fact that India has yet to join the Optional Protocol to the International Covenant on Civil and

[13] K.S. Puttaswamy v Union of India, W.P. (C) NO. 494/2012

ISSN: 2582-6433

Political Rights or subscribe to the Organisation for Economic Cooperation and Development guidelines, it did indeed affirm the International Covenant on Civil and Political Rights on the tenth day of April in the year nineteen hundred and seventy-nine. This manifestation of commitment obligates member states to maintain and preserve Article 17, guaranteeing the preservation of the fundamental right of privacy. Additionally, multiple instances exist in which India's Supreme Court has utilized laws of an international character in a plethora of cases that lacked any domestic counterpart or regulation. It must be said that the Supreme Court has confirmed that international conventions and dictums must operate in conjunction with the fundamental human rights consigned in Part III of the Indian Constitution, provided no form of locally-enacted legislation exists, and there is no friction detected between them. In the form of the Information Technology (Amendment) Act of 2008 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules of 2009, India has passed legislation controlling mass surveillance ventures that necessitate the interception of communicative messages. Nevertheless, these surveillance operations have been instigated without judicious analysis or scrutiny. In October 2012, a task force led by Justice AP Shah circulated an extensive report that encompassed privacy laws in a variety of forums. Said report aimed to present recommendations concerning the right to privacy, specifically in response to the expansion of state and corporate surveillance capabilities in the age of digital revolution.

Unveiled by the report, a specified set of nine National Privacy Principles have been identified as the directive intended to furnish guidelines and procedures when it comes to the acquisition, handling, storage, maintenance, access, distribution, disposal, and anonymization of sensitive personal information, personal identifiable information, sharing, transfer, and identifiable information. To further fortify the privacy of all individuals concerned, regardless of their origin, against any potential violations committed by governments, public entities, or private companies, the Privacy (Protection) Bill was ratified in 2013, recognizing the rights of individuals whose data is being processed. However, it appears that the Bill is not clear on the definition of the term "informed consent." Moreover, the bill does not account for video surveillance cameras (CCTV), nor does it mention a set of guidelines for the use of mobile camera users. Intrusion monitoring technologies have no said restrictions imposed upon them, and the draft law in place does not provide sufficient definitions of "public order" or "prevention of incitement to crime." Thus, the law enforcement agencies are

ISSN: 2582-6433

bestowed with enormous power to intercept anyone's communication, without grounds for probable cause. To intercept the communication, the entire mechanism necessitates forensic discovery. Unregulated surveillance is probably one of the most critical threatening factors to our right of privacy that is being grossly overlooked.[14]

- **ROAD AHEAD**

As a nation boasting one of the largest democracies on earth, our duty to empower our citizens toward their rights and preserve national security cannot be overstated. When it comes to national security and privacy, these two interests have been traditionally viewed as oppositional in nature. However, with the advent of advanced technologies and digital surveillance capabilities, safeguarding citizens' information has become equally as critical as national security itself. It is, in fact, the optimum time to explore the idea of recognizing the protection of citizens' privacy and information as an integral facet to preserving national security. As of late, governmental legislation highlights, including the alterations made to the IT Act 2000 via the IT Rules 2021, and the broad exemptions afforded to government and allied organizations under the proposed Data Protection Bill 2021, have increasingly catered to policies that either omit or weaken privacy measures afforded to citizens, rather than placing significant emphasis on establishing privacy-respecting practices for all. Regrettably, the often-overlooked outcome of adopting these methods is that the privacy and security of law-abiding citizens are frequently compromised. One such example of the resultant breach is that the IT Rules mandate originator traceability, likely interfering with encrypted communication and adding unprecedented vulnerabilities to other services readily exploitable by unscrupulous parties.

To mitigate issues such as these, it is imperative that we overhaul the Indian surveillance framework in its entirety, instead of adopting broad mandates or imposing privacy-infringing policies. The contemporary framework proving entirely outdate poses one of the fundamental challenges to employing more advanced security strategies and digital surveillance techniques. A new framework, therefore, must put in place a precise, purposive, proportionate, and comprehensive system, with

[14] Addison Litton, The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-expression, 14 WASH. U. GLOBAL STUD. L. REV. 799 (2015), https://openscholarship.wustl.edu/law_globalstudies/vol14/iss4/17

ISSN: 2582-6433

privacy-respecting practices as the norm across the board. Currently, our system faces numerous obstacles that must be tackled with urgency. The crux of the issue lies in the terminology used in our legislations, which is ambiguously defined and offers little clarity on the scope of intended purposes for surveillance activities. Such loose definitions have allowed intrusive surveillance practices to be employed outside the intended boundaries. To tackle this issue, our system must emphasize accountability mechanisms through judicial or parliamentary oversight and establish appropriate procedural safeguards. This would greatly reduce the wide-ranging discretionary powers of state actors who currently possess the ability to exercise extensive surveillance powers.

ISSN: 2582-6433

CHAPTER IV: CONCLUSION AND SUGGESTIONS

- **SUGGESTIONS**

Surveillance of any kind should be conducted by independent, impartial, and competent authorities. Although the policy recommends that the authority be the judiciary, the realities of the Indian judiciary and the need for an often immediate response to permission requests raises the question of whether judges are the best institution to confer these powers

In all cases of surveillance, the law must require that, before issuing a surveillance order, it must be determined and demonstrated that:

- There is a high likelihood that a serious criminal offense has been or will be committed.
- Other available, less intrusive investigative techniques have been exhausted, information access is limited to information reasonably relevant to the alleged offence, and any excess information collected is properly destroyed or returned. The information will only be accessed by designated authorities and will be used for the purposes for which it has been granted if
- Monitoring is necessary to achieve legitimate goals
- All authorities responsible for authorizing surveillance must have the knowledge and capacity to make decisions about the legality of surveillance, the use of such technologies and the human rights implications.
- Law enforcement can only collect relevant information such as specified in a statutory order
- Information collected that is not related to the stated Legal purpose, should be destroyed or a new license to use the information should be obtained
- Information should be only used for the purposes specified in the lawful order
- Allow Individuals to Participate in the Fair and Public Hearing Process

In India's surveillance system, anyone who fails to comply with an interception, monitoring, or decryption order can be held accountable and penalized with up to seven years in prison. Similarly, noncompliance with an order related to the collection of traffic data could result in a prison sentence of up to three years. These penalties are not proportional to the offense committed and do not encourage service providers to resist or challenge unauthorized or potentially illegal surveillance requests. In alignment with the Necessary and Proportionate principle of safeguards against

ISSN: 2582-6433

unwarranted access, it is recommended that service providers be allowed to deny requests that are not legally approved without fear of imprisonment. Furthermore, it is suggested that the Indian surveillance regime impose penalties that are commensurate with the severity of the offense, and that intermediaries not be penalized for questioning the legality of requests. The surveillance system in India lacks transparency measures. As a result, the information that the public receives regarding the government's surveillance practices is either unofficial or based on leaked data.

To ensure transparency and public oversight, it is suggested that the Indian surveillance regime includes the following mechanisms of transparency and accountability, which are necessary and proportionate principles.

- Being open and clear about the application and extent of communication strategies is crucial.
- The laws that allow for communications surveillance should be transparent.
- The requirements in regards to surveillance of communications that service providers need to adhere to should be transparent and clearly defined.
- Whenever feasible, the procedural aspects of surveillance, including the delegation of surveillance authority to various entities, should be made transparent.
- The development of new surveillance schemes and powers by authorities and departments.
- The procurement and enhancement of surveillance technology.
- In order to promote transparency, service providers should be permitted to publicly disclose the protocols they use when handling state communications surveillance.
- In order to ensure transparency and accountability in regards to communication surveillance, it is imperative that an independent oversight mechanism is established. This mechanism will ensure that the Indian Government is being transparent and accurate in its publication of information about the use and extent of communications surveillance techniques and powers. It is important to note that this oversight mechanism should be supplementary to any existing oversight provided by other branches of government.

ISSN: 2582-6433

- ## CONCLUSION

As we embark on the journey of newer technologies such as Web 3.0 and elevate the degree of digital penetration in India, the government's regulatory priorities must comprehend the pivotal requirement of restructuring the framework governing surveillance. A deeper deep-dive into the need for profound consideration of an overhaul of the legal framework of targeted surveillance (micro-level) should lead us to converse about other facets such as mass and lateral surveillance, which are currently not at all delineated by any articulated legal framework. For instance, there has been an inundation of reports on drones with cameras being utilized for monitoring purposes where we don't know the use of the recorded videos yet. The information on the individuals being scrutinized through these audio-visual tapes is happening in parsimonious silos without defining terms like suspects or suspicious activities, etc., which is an outrageous violation of the principles of equitable justice. Additionally, in most cases, individuals hardly become aware of the data collection and profiling practices happening through these digital surveillance tools, gravely compromising their privacy. Hence, we hope that augmenting the need for a resolute remodelling of the framework governing targeted surveillance will trigger a much-needed conversation on laying the robust foundations to establish new legal reforms for a harmonious balance between privacy and national security with other forms of surveillance. Constitutional principles require government supervision to be properly carried out within a certain range. The K.S. Puttaswamy v. Union of India Supreme Court decision reinforced a citizen's right to privacy, particularly informational privacy, and mandated any infringement on these rights to be done within the bounds of proportionality, legality, and necessity. In another judgment, the Manohar Lal Sharma vs Union of India (the Pegasus case) established a group of experts to recommend changes to the current laws around surveillance, with the aim of securing each citizen's right to privacy.

The need to regulate surveillance activities, particularly those pertaining to privacy, is even backed by judicial support in India. Recent events such as Pegasus snooping and face recognition technology have left the public distrustful of surveillance methods without adequate legislation and safeguards in place. The significance of surveillance regulation goes beyond the local level and has potentially far-reaching implications, even on digital trade. Jurisdictions now evaluate the level of privacy protection afforded to data within other jurisdictions when arriving at data flow arrangements. As such, surveillance regulation must be approached with great care and be mindful of the implications of our decisions

ISSN: 2582-6433

BIBLIOGRAPHY

1. A Comprehensive Note On INDIAN CONSTITUTION- A source code to billion dreams, https://loksabhadocs.nic.in/Refinput/Research_notes/English/04122019_153433_1021204140.pdf
2. A TYPOLOGY OF PRIVACY BERT-JAAP KOOPS, BRYCE CLAYTON NEWELL, TJERK TIMAN, IVAN ŠKORVÁNEK, TOMISLAV CHOKREVSKI, AND MAŠA GALIČ, Published by Penn Law: Legal Scholarship Repository, 2017, https://scholarship.law.upenn.edu/jil/vol38/iss2/4
3. Addison Litton, The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-expression, 14 WASH. U. GLOBAL STUD. L. REV. 799 (2015), https://openscholarship.wustl.edu/law_globalstudies/vol14/iss4/17
4. Alan F. Westin, *Privacy And Freedom*, 25 WASH. & LEE L. REV. 166 (1968). Available at: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20
5. Human Rights Instruments CORE INSTRUMENT UNIVERSAL INSTRUMENT Optional Protocol to the International Covenant on Civil and Political Rights ADOPTED 16 December 1966 BY General Assembly resolution 2200A (XXI), https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-international-covenant-civil-and-political
6. Privacy, free expression and transparency Redefining their new boundaries in the digital age Joseph Mifsud BonniciEvgeni Moyakine Published in 2016 by the UNESCO 2016ISBN 978-92-3-100188-8, http://creativecommons.org/licenses/by-sa/3.0/igo
7. Privacy: practical controversies, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 83–222 (Beate Roessler & Dorota Mokrosinska eds., 2015). https://doi.org/10.1017/CBO9781107280557
8. Dr. G. Mallikarjun and B. Md. Irfan, Right to Privacy in India: The Technical And Legal Framework
9. Rabindra Kumar Mohanty. (2011). David Lyon, Surveillance Studies: An Overview, Polity: Cambridge, 2007; 256 pp.: ISBN 9780745635910, £55.00 (hbk), ISBN 9780745635927, £14.99 (pbk). International Sociology, 26(2), 284–284. https://doi.org/10.1177/0268580911026002 2003
10. The "Criminal Tribe" and Independence: Partition, Decolonisation, and the State in India's Punjab, 1910s-1980s Sarah Eleanor Gandee, The University of Leeds and Sarah Eleanor Gandee August 2018 https://etheses.whiterose.ac.uk/22408/1/Gandee_SE_History_PhD_2018.pdf