SUPREMO AMICUS

VOLUME 32 | JANUARY, 2023 ISSN 2456-9704

NATIONAL SECURITY AND SURVEILLANCE LAWS: AN INFRINGEMENT OF THE RIGHT TO PRIVACY?

By *Prerita Bhardwaj*
From Symbiosis Law School, Pune

Abstract

In India, these are challenging times for the right to privacy. The government is adopting programmes that will result in the establishment of nationwide databases of personal information. The idea of surveillance has evolved, and a plethora of digital monitoring methods used by governments worldwide, most notably in India, have normalised the transition away from targeted surveillance toward random mass surveillance. Prioritizing 'national security' above individual liberty seems to be a widely accepted practise used to justify monitoring. This article examines how national security is regarded in India, where security legislation and associated discourses focus on defending the state against actual or perceived challenges to its survival, rather than on defending people against real or perceived dangers to their safety. As a result, the need of strengthening our present privacy measures to meaningfully preserve the right to privacy in the face of governmental monitoring is discussed.

Keywords: *Right to Privacy, National Security, Surveillance.*

INTRODUCTION

In today's digital culture, both the right to Privacy and right to information are critical human rights. These rights complement one another in terms of making governments responsible to citizens. However, when a request to disclose personal information stored by government entities is made, a contradiction between these rights may arise.

New technology and activities are posing a growing threat to Privacy. Personal data is being collected and shared at an increasing rate as a result of technological advancements. Sensitive personal information (like biometrics) is now regularly gathered and exploited.

Simultaneously, the public's right to knowledge is gaining widespread acceptance. RTI laws are now widespread around the globe, having been enacted in almost 90 nations. Individuals have a fundamental human right to demand information kept by government entities. The fundamental purpose of the Right to Information Act is to empower citizens, to encourage openness and integrity in government operations, and to make democracy really function for the people. The right to information is essential for participatory democracy to function properly - it is required to promote accountability and effective governance. The Right to Information is drawn from Article 19 (1) (a) of the Constitution's fundamental right to freedom of speech and expression as held by the landmark case **Bennett Coleman and Co. v. Union of India**.[1]

While the Right to Privacy has been lifted to the status of a fundamental right, it is not an

[1] Bennett Coleman and Co. v. Union of India, AIR 1973 SC 106

absolute right. It is susceptible to some constraints or limitations, such as those imposed for national security purposes. Similarly, various countries' RTI laws have Exemptions that permit the withholding of specific kinds of information. Among these exceptions is the safeguarding of national security.[2]

We have seen a slew of Privacy and personal data collecting concerns over the previous decade, beginning with the Snowden revelations, Cambridge Analytica, Whatsapp's privacy policy, and the Aadhar case. In light of recent discoveries on surveillance and Privacy, this paper will attempt to examine the current status of privacy laws in India and the topic of privacy protection.

EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA: A JUDICIAL CONSTRUCT

What is Privacy?

Privacy is the most treasured right in our society and is necessary for human life. Liberal scholars such as John Locke, Jurgen Haberman, and John Rawls have maintained that the home, family, personal places, and relationships must be preserved and kept separate from the state and society.[3] According to Article 12 of the Universal Declaration of Human Rights, no one should be submitted to unlawful intrusion with his or her private, family, home, or communications, or to assaults on his or her dignity or reputation.[4] Every individual has a right to be protected from such interference or assault. The same is reiterated in Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[5] and the European Convention on Human Rights[6].

Judicial Pronouncements and Legislations with the aspect of Privacy

In India, the right to Privacy is derived largely from Article 21[7] of the Indian Constitution, which declares that no individual shall be stripped of his life or personal liberty unless in accordance with the legal process. While the Indian Constitution does not expressly acknowledge the right to Privacy as a fundamental right, it is implied in terms of Article 21 of the Constitution, as shown by court decisions.

However, if one examines several legislations in our nation to ascertain the status of the notion of Privacy, one will discover multiple measures adopted to safeguard it. For instance, Sections 28 and 29 of the Criminal Procedure Code, 1973, Section 509[8] of the Indian Penal Code, 1860, among others, have the aspect of privacy protection. Additionally, in Dharam's ancient law, Shastras acknowledged the notion of Privacy.

As per Supreme Court rulings, Privacy is a fundamental right that needs constitutional safeguarding. Its evolution is traced through the following landmark judgements. In **Nihal**

[2] MP JAIN, INDIAN CONSTITUTIONAL LAW, 1063 (LexisNexis 2018)
[3] B Acharya, *The Four Parts of Privacy in India.* Economic and Political Weekly, 32-38 (2015).
[4] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: https://www.refworld.org/docid/3ae6b3712c.html [accessed 7 March 2022]
[5] International Covenant on Civil and Political Rights, art. 17, Apr. 16, 1966, United Nations, Treaty Series, vol. 999, p. 171.
[6] European Convention on Human Rights, Art. 8, 4 November 1950, ETS 5
[7] INDIA CONST., art. 21
[8] Indian Penal Code, § 509, 1860, No. 45, Acts of Parliament, 2000 (India

Chand v. Bhagwan Dei,[9] the Allahabad high court made the initial move to recognize the Right to Privacy as a self-contained entity that derives from the people's customs and traditions and is a legislative right. The Supreme Court first reviewed whether the 'right to Privacy is a fundamental right in **M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors**.[10] The warrant granted for search and seizure under Sections 94 and 96 (1) of the Code of Criminal Procedure was questioned. The Court declared in **R. Rajagopal and Anr. v State of Tamil Nadu**[11] that Article 21 contains an implied right to Privacy, which is construed as the right to be left alone. In the **K.S. Puttaswamy**[12] case, the Supreme Court unanimously held that the right to privacy is an integral aspect of the right to life and personal liberty guaranteed by Article 21.

RELATIONSHIP BETWEEN PRIVACY OF CITIZENS, RIGHT TO INFORMATION AND NATIONAL SECURITY

National Security: An elusive term

National security has been defined as a state's capacity to protect and defend its citizens.[13] National security issues are often classified and sensitive and thus are not brought to light in order to account for the terror that individuals may have. A danger to national security jeopardizes the safety of people, necessitating severe measures to safeguard them. Terrorism, espionage, and military coups are only a few examples of risks to national security.[14] To put a stop to these kinds of threats, the government determines that emergency legislation and military tactics are essential to assist in restoring national peace and stability. However, there are situations when the basic rights of citizens might be arbitrarily revoked. The announcement of a danger to national security vests the government with a considerable deal of authority, and the potential for abuse is high. Since the mid-twentieth century inception of the human rights movement, the advancement of human rights has been viewed as conflicting with or even jeopardizing fundamental national security concerns.[15]

Therefore, in terms of national security, states continue to cling to a notion that is famously elusive and seems to be in clear opposition with the protection of human rights. The term national security is elusive because despite being established as a justified limitation on fundamental rights, the word "national security" remains vague and devoid of judicial scrutiny.[16]

The misuse of this word by the government is apparent from the recent RTI reports which state that RTI applications denied due to

[9] B. Nihal Chand and Another v. Mt. Bhagwan Dei, 1935 AWR 1109

[10] M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors, 1954 AIR 300,

[11] R. Rajagopal and Anr. v State of Tamil Nadu, 1995 AIR 264

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

[13] **National Security versus Global Security, Segun Osisanya, UNITED NATIONS,** https://www.un.org/en/chronicle/article/national-security-versus-global-security

[14] Shruthi Raghavan, *Trade-off between a Citizen's Right to Privacy and National Security*, 2 Supremo Amicus 355 (2017).

[15] William W. Burke-White, *Human Rights and National Security: the Strategic Correlation*, 17 HARv. HUM. RTS. J. 251(2004).

[16] K.G. KANNABIRAN, THE WAGES OF IMPUNITY: POWER, JUSTICE AND HUMAN RIGHTS 4 (Orient Blackswan Private Limited 2004)

national security concerns have increased by 83 percent in 2020-21.[17]

The notion of National Security in India in comparison on International Level

In India, the notion of national security is perceived in its traditional realist sense wherein security connotes "territorial integrity".[18] In this kind of system, security regulations and associated national security frameworks are designed to safeguard the state against actual or perceived risks to its survival, rather than to safeguard individuals against genuine or apparent dangers to their well-being and security.[19]

As compared to the positive stance articulated in some international agreements, India's approach to the 'national security' concept looks to be regressive and obsolete.[20] An example of such an international agreement is the Johannesburg Principles on National Security, Freedom of Expression, and Access to Information. As per Principle 2 of the principles, a limitation is not valid except if serves to safeguard a nation's "existence or territorial integrity against the use or threat of force,"[21] or its capability to retaliate to force, from potential danger. Additionally, the Siracusa Principles on Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights lay down that national security must not be invoked to justify the imposition of ambiguous or unreasonable restrictions. They may be used only when appropriate measures and adequate remedies against misuse are in place.[22]

SURVEILLANCE FOR NATIONAL SECURITY: A THREAT TO PRIVACY?

Surveillance is the term used to describe the careful observation of a person or organization, particularly one suspected of being monitored.[23] When it comes to State Surveillance, there are numerous conflicting parties at stake such as Government interest, Public good, and Individual interest. The Judiciary must use a deft judgment method in order to strike a balance between all three while maintaining stability.

The rapidly growing surveillance system involves the government, technology corporations, and individuals, who may work together to watch people. While people being seen are constantly exposed, the observers stay impenetrable. This raises the likelihood

[17] MINT, https://www.livemint.com/news/india/rti-applications-rejected-over-national-security-up-83-in-2020-21-report-11646472679235.html (last accessed March 8, 2022)

[18] Prakhar Bhardwaj & Abhinav Kumar, *Comparing Two Inchoate Conceptions: Balancing Privacy and Security by E-Surveillance Laws in India*, 3 NAT'l L.U. DELHI Stud. L.J. 1 (2014).

[19] Asmita Basu, *Routinization of the Extraordinary- a Mapping of Security Laws in India* (2009), http://www.southasianrights.org/wp-content/uploads/2009/10/IND-Security-Laws-Report.pdf

[20] Supra, Note 17

[21] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Principle 2, 1 October 1995, available at: https://www.refworld.org/docid/4653fa1f2.html [accessed 8 March 2022]

[22] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4, available at: https://www.refworld.org/docid/4672bc122.html [accessed 8 March 2022]

[23] Chhaya S Dule et al, *Analyze The Legislative Framework relating to Surveillance and Right to Privacy: Issues and Challenges,* ICRAEM, 981, (2020)

of rights breaches, particularly the historically neglected right to be free from hidden monitoring and to have one's information protected.[24]

Legislations

Analysing legislations shows that some clauses give surveillance power to the government. The Indian Telegraph Act of 1885 empowered the government with surveillance authority. Colonial law empowered both state and central administrations to intercept letters that posed a danger to the state's sanctity. Similarly, Section 69 of the Information Technology Act 2000 exempts information from privacy protection if the substance of the information jeopardises India's sovereignty or jeopardises the state's security in any manner.[25] According to Rule 3 of the IT Rules 2009 (process and safeguards for information interception, monitoring, and decryption), no person may intercept, track, or decrypt information unless according to a direction issued by a competent authority.[26]

Law on Privacy through Case Laws

Kharak Singh v. State of Uttar Pradesh[27] marked the beginning of the modern era of Indian law on privacy and surveillance. In this case, the police surveillance included secret picketing of the suspect's house, the use of inquiry slips, and constables reporting the suspect's movements, among other things. All of this information is recorded and forwarded to the appropriate superior officer. The Court has invalidated regulation 236(b) of the UP police act for violating Article 21's guarantee to personal liberty. Justice Subba Rao stated that wide surveillance rights jeopardise the safety of innocent persons and that the right to privacy is a necessary component of human liberty, thereby he held all surveillance measures unconstitutional.[28]

Following Kharak Singh, the Supreme Court declared in **Gobind v. State of M. P**[29] that the right to privacy was derived from Articles 19 and 21. The **People's Union for Civil Liberties (PUCL) v. Union of India**[30] is the most essential case after the Gobind Singh case. The Supreme Court in this decision established specific procedural safeguards for conducting legitimate interceptions and also established a high-level review body to determine the significance of such interceptions. However, such prudence has been chucked in recent government instructions, as seen by the phone tapping events which have surfaced.

The Puttaswamy Case[31] expressly acknowledged the right to informational privacy. Individuals have the inherent right not to be pressured into consenting to a state welfare scheme. This argument was succinctly stated by Justice Kaul, when he said that the Government must guarantee that data is not utilised without the users' consent

[24] Digital Surveillance and the Threat to Civil Liberties in India Author(s): Sangeeta Mahapatra German Institute of Global and Area Studies (GIGA) (2021) Stable URL: https://www.jstor.org/stable/resrep31794 Accessed: 06-03-2022 14:33 UTC

[25] Information Technology Act 2000, § 69, No. 21, Acts of Parliament, 2000 (India).

[26] **Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 3**

[27] Kharak Singh v. State ofU.P., AIR 1963 1295

[28] Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, 26 NAT'l L. Sch. INDIA REV. 127 (2014).

[29] Gobind v. State of M.P., AIR 1975 SC 1378.

[30] People's Union for Civil Liberties (PUCL) v. Union of India, AIR 1997 SC 568

[31] *Supra,* Note 12

and is utilized for the intent and scope for which it was supplied.

State Surveillance in India

Since the catastrophic Snowden leaks in May 2013, worldwide debates about state monitoring and people's right to privacy have been in the limelight.

Despite the various Supreme Court rulings that reaffirm the concept of right to privacy, surveillance is carried out in a number of methods nowadays, including wiretaps, GPS monitoring, email and message decryption, and tracking internet and social media activity. Mass communication interception, keyword searches, and simple access to specific individuals' data all indicate that the state is headed toward unrestricted large-scale communication surveillance. Through numerous surveillance measures, the Indian government has recently expanded the scope of the surveillance system like Central Monitoring Scheme (CMS), the Crime & Criminal Tracking Network & Systems and NATGRID. The Aadhar, a nationwide biometric identification system implemented by the Indian Government also deserves mention here.

While national security is the foremost reasoning for surveillance in India and may be well-intentioned, India should prioritise strengthening its national security through stronger privacy protections.

CONCLUSION

The contemporary era is defined by a struggle between the interests of security and the right to privacy. While the Constitution recognises the right to privacy, its growth and development are completely at the discretion of the court. National security is an umbrella word, and the term's arbitrariness has resulted in the specific targeting and tracking of individuals in a number of countries. The use of spy software for monitoring and surveillance has a chilling impact on the right to freedom of expression, particularly at a time when political activists and academics are being arrested for voicing alternative views. Without defined limitations, there is no difference between data collection and state-sponsored surveillance, and the usage of a blanket term such as national security creates uncertainty about what constitutes a threat to the state.

It is imperative that clear parameters for the same are formulated and strengthening of national security through stronger privacy protections is prioritised by the government and viewing the concept of national security in a more progressive way as enshrined in the siracusa and Johannesburg principles and Justice Hidayatullah's concentric circles analysis.[32]

Therefore, governments must provide stronger protections for private privacy, since they are the primary perpetrators of breach in this situation, and undermining the authority of the government may be considered as a blatant attack on the constitutional concepts of liberty, dignity, and fraternity.

*****

[32] . M. Lohia v. State of Bihar, A.I.R. 1966 S.C. 740; Dropti Devi v. Union of India & Ors, A.I.R. 2012 S.C. 2550

VOLUME 32 | JANUARY, 2023 ISSN 2456-9704