Page 1450 - 1459 **DOI:** *https://doij.org/10.10000/IJLMH.115907*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 5

2023

Surveillance: Is it a Threat to Privacy

M.K. GURU PRASATH[1] AND V. HARI CHARAN[2]

ABSTRACT

In an era characterized by rapid technological development, surveillance has become an integral part of modern societies. This study aims to critically examine the potential threats that surveillance may pose to privacy in India. The paper uses a multidimensional approach to analyze the complex interaction between surveillance practices and privacy concerns, taking into account legal, ethical and socio-political aspects.

The study first examines India's legislative framework for surveillance, highlighting the role of legislation and the judiciary in protecting individuals' privacy rights. It deals with regulations such as the Information Technology (IT) Act, 2000, which regulates cyber surveillance and the right to privacy under the Indian Constitution. Assessing relevant jurisprudence, this brief analyzes the extent to which existing laws effectively protect privacy in the face of evolving surveillance technologies.

In addition, this study also explores the ethical implications of surveillance practices in India. This raises questions about the balance between the security interests of the state and the protection of citizens' privacy.

Keywords: *Surveillance, Privacy, Indian Constitution, IT Act.*

I. INTRODUCTION

Privacy is a basic human right which has been recognized in international laws and constitution of various countries. Though it is not explicitly mentioned in the Indian Constitution, the Indian Judiciary has recognized the right to privacy as fundamental right under Article 21 of the Indian Constitution. It is crucial for self-expression and individuality. On the other hand, the Surveillance is an essential tool for maintaining the sovereignity, integrity and security of the state. It prevents the threats to the national security such as terrorism and espionage. It also used to investigate and detect crimes. However, if the surveillance is conducted without transparency it infringe the privacy of individuals. There lies a change in balancing between these competing interests.

(A) Right to privacy:

The right to privacy means “right to be left alone”. It is a fundamental right which enables the

[1] Author is a student at the Tamil Nadu Dr. Ambedkar Law University, School of Excellence in Law, India.
[2] Author is a student at the Tamil Nadu Dr. Ambedkar Law University, School of Excellence in Law, India.

 [ISSN 2581-5369]

individuals to keep personal information and gives protection against unwarranted intrusion by others including the government. It safeguards one's personal space from unauthorized surveillance. It is a basic component of individual autonomy and personal freedom. It includes:

i. Right to control personal information

ii. Right to maintain personal space

iii. Right to make personal choices

iv. Right to protect dignity

v. Right to secure communications

In 1954, Eight Judge bench of the Supreme Court of India held that thee is no right to privacy enshrined in Indian Constitution [3]. But, it was overruled in Kharak Singh Case.

In case of Kharak Singh v. State of Uttar Pradesh[4], The petitioner has been charged for dacoity but he was released due to lack of evidence. However, the police opened history sheet against him on basis of accusation. Under regulation 236 of chapter 20 of U.P. Police Regulations, police conducted the surveillance by frequent visit his house, tracking his movements and periodic inquires. He challenged the U.P. Police Regulations on the ground that the surveillance violated his fundamental rights which are guaranteed under Article 14 and Article 21 of the Indian Constitution. The court struck down the regulation as unconstitutional on the ground it violates Article 14 and Article 21. It further held that "right to privacy" fall within the ambit of personal liberty under Article 21 of the Indian Constitution.

In the case of Justice K.S. Puttuswamy v, Union of India[5],The Constitutional validity of Aadhar based biometric system was challenged before the hon'ble supreme court. Where it was held that the right to privacy is an intrinsic part of right to life and personal liberty which is guaranteed under Article 21 of the Indian Constitution.

In the case of Manohar Lal Sharma v. Union of India,[6] The court held that the right to privacy which is guaranteed under Article 21, has been manifested in the multiple facets in the personal and public lives of the citizens of India.

(B) Surveillance:

According to Webster dictionary, Surveillance means "keeping a close watch on someone or

[3]M.P. Sharma v. Sathish Chandra, AIR 1954 SC 300
[4] 1964 SCR (1) 332
[5] (2017) 10 SCC 1
[6]Writ Petition No. 314 of 2021

 [ISSN 2581-5369]

something"[7]. It refers to the systematic monitoring the activities of individual or group of individuals for the purpose of gathering information. It can take varieties of form such physical observation, electronic monitoring, video recording, etc. Surveillance is critical to maintaining public safety. It helps law enforcement agencies detect and prevent crime, identify potential threats, and respond to emergencies. In digital age, surveillance plays an important role in safeguarding sensitive data and information from cyber attacks.

II. LAWS GOVERNING SURVEILLANCE

In India, surveillance is governed by several laws and regulations which are follows:

1. Indian Telegraph Act, 1885

Indian Telegraph Act majorly with the interception of calls. It is an legislation which governs the use of wired and wireless telegraphy, radio, digital data communications. Its gives jurisdiction to government of India to establish, maintain, operate and oversight of all types of wired or wireless communications within the territory of India. It also provide authorization to government law enforcing agencies to intercept communication and tapping of phone lines under the conditions defined in the constitution of India

Section 5(2) of this act which expresses that on the off chance that any open crisis or in the perspective on wellbeing of public, or in light of a legitimate concern for public the focal or state government or some other authority for the focal or state government is fulfilled that in the sovereignity and respectability of India, security of nation or to forestall any offense it is important to do so then, at that point, by the motivations to be kept recorded as a hard copy that message or any class of messages to or from any individual got by any message will not be communicated, caught or confined or will be uncovered to government.

In the case of People Union for Civil Liberties v. Union of India[8], The constitutional validity of section 5(2) of Indian Telegraph Act was challenged. The court observed that right to hold telephone conversation without any interferences fall within the ambit of right to privacy. Therefore, telephone tapping is violation of Article19 (1) (a) and Article 21 of the Indian Constitution. In Vinit Kumar v. Central Bureau of Investigation[9],The court observed that An order of interception under section 5(2) of the IT Act can only be given in situations of 'public emergency' or 'public safety'.If interception has been undertaken in contravention of Section 5(2) of the IT Act, it is mandatory for the said intercepted messages to be destroyed.Evidence

[7]Surveillance, Merriam-Webster Dictionary (11th edition, 2003)
[8]AIR 1997 SC 568
[9] 2019 SCC Online Bom 3155

 [ISSN 2581-5369]

procured in violation of Section 5(2) and the rules made thereunder, is not admissible in court.

2. Information Technology Act, 2000

IT Act mainly deals with cyber crime and electronic commerce. The relevant legal act was prepared for the legal recognition of transactions made through electronic communication and data storage. It deals with crimes involving a computer or network located in India.

Section 69 of the Information Technology Act and the Information Technology (Security Measures for Interception, Monitoring and Decryption of Data) provisions were introduced in 2009, which promoted the legal framework for electronic surveillance. Under this law, any electronic communication can be intercepted. Section 69 of the Information Technology Law expands the surveillance in addition to the limitations provided in the Telegraph Act and Articl 19 (2)of the Constitution, which means that the surveillance activity can also be used in the investigation of a crime.

3. Information Technology (Procedure and Safeguard for Inception, monitoring and decryption of Information) Rules, 2009:

The central government has passed Information Technology (Procedure and Safeguard for interception, monitoring and decryption of information) Rules, 2009 in which it was laid down that no person shall intercept, monitor or decrypt any information available on any computer resources except an order from Home Secretary or Joint Secretary, Ministry of Home Affairs has been obtained to do so. According to Rules, under Rule 4, it has been laid down that the central government has power to delegate such authority to intercept, monitor or decrypt any information on any computer resource to any agency.

Information by Public) Rules, 2009 has been passed by parliament in order to block access of any information on any computer resource by public. According to Rules, the government has power to block any information whether generated, transmitted, stored or received or hosted by any computer resource for any reasons mentioned in section 69A of the Information Technology Act, 2000 i.e. sovereignty and integrity of India, defense of India, friendly relation with foreign state, security of state etc.[10]

4. Right to Privacy Bill, 2011

The bill states that "everyone has the right to privacy - the confidentiality of his communications, including personal correspondence, telephone conversations, telegraphic

[10] Prashanti Upadhyay, Surveillance in India and its Legalities, https://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html (Last Visited at Aug, 26, 2023)

 [ISSN 2581-5369]

messages, mail, emails and other means of communication; his private or family life; protection of his honor and good name; protection against search, seizure or disclosure of lawful communications between individuals; privacy from surveillance; confidentiality of one's banking and financial transactions, medical and legal information, and protection of personal information".The bill provides for the creation of a Central Communication Interception Review Committee, which will be given the authority to review all orders for communication interceptions and determine whether they violated Section 5 of the Indian Telegraphs Act, at which point the material should be immediately destroyed. Additionally, except in specific circumstances and in accordance with the prescribed procedure, it is illegal to observe another person by the use of closed-circuit television, another electronic device, or any other method.

5. Aadhar Act, 2016

This Act governs the use of Aadhar, India's Biometric System. The main purpose of the act is to provide a unique identification number every resident of India. It aims at eliminating fake identities and helps to protect privacy and prevents unauthorized use.

6. Personal Data Protection Bill 2019

A Joint Parliamentary Committee is currently reviewing this law, and experts believe that it is biased in the government's favor and is detracting attention from individual privacy as a result of recent observations. After two years of deliberation, the Joint Parliamentary Committee adopted its report, which included a number of improvements and amendments, including the request to rename the legislation the "Data Protection Bill" and eliminate the word "personal." It suggests that both personal and non-personal data should be governed by the same agency.

III. INDIAN JURISPRUDENCE OF RIGHT TO PRIVACY

The Right to Privacy is not explicitly stated in the Constitution of India. The right to Privacy is neither a fundamental right nor a constitutional right. The Right to Privacy was a right which was formed in the field of Tort Law. The Right to Privacy has never been listed as a fundamental right and has always been a subject of interpretation by the judiciary.

The 1954 case of MP Sharma v. Satish Chandra[11] was the first case which dealt with the question of privacy. This was the foremost judgement in the Indian Jurisprudence which dealt with the Right to Privacy. In this case, the petitioner challenged the constitutionality of the provision which provides for the search and seizure of documents from a person against whom a FIR had been lodged. The Court was put in a position to decide whether such a provision

[11]AIR 1954 SC 300.

 [ISSN 2581-5369]

would in anyway breach the Right to Privacy and whether such a provision was unconstitutional. The Supreme Court held that the right to privacy was not a fundamental right guaranteed by the Indian Constitution. The court held that the Right to Privacy was not an absolute right and there can be reasonable restrictions on the Right to Privacy. So, it was decided that the provision was a reasonable restriction on the right to Privacy and so the provision was not unconstitutional.

In 1962, in Kharak Singh v. State of UP[12], the court examined the question relating to the power of Police in surveilling the acquitted criminals. In this case, the petitioner was a dacoity accused who was acquitted by the court, citing lack of evidence for conviction. However, the Police officials regularly surveilled him, thereby infringing his Right to Privacy. So, the petitioner claimed to enforce his right under Article 21. But, the court following its previous decision in MP Sharma v. Satish Chandra, ruled in favour of the Police, saying that the Right to Privacy is not an absolute fundamental right guaranteed by the Constitution.

Both the above rulings followed the law set by the Supreme Court in A.K. Gopalan v. The State of Madras[13]. In this case, the court held that the Right to Privacy is ensured only according to 'procedure established by law'. It means that Right to Privacy can be claimed only if the infringement is not according to law, i.e, the provisions of the legislation or statute.

However, the ruling of AK Gopalan v. State of Madras was overruled in Maneka Gandhi v. UOI, where the scope of Article 21 was broadened. This paved the way for an essential change in the jurisprudence of Right to Privacy in India.

The first case where the Apex court ruled the Right to Privacy as a Fundamental Right was the case of Gobind v. State of MP[14]. The Supreme Court held that the right to privacy arises from both Article 21 and Article 19, the freedom of speech and movement. The court further observed that the right to privacy included "personal intimacies of the home, the family marriage, motherhood, procreation and child bearing". However, the Supreme court held that Right to Privacy is not an absolute right and is subject to Procedure established by Law, i.e., Due process of Law. The court in R. Rajagopal v. State of TN[15], held that the violation of the right to privacy is a violation of Fundamental Rights of an individual.

Later in 1997, in the case of PUCL v. UOI[16], popularly known as the telephone tapping cases,

[12]AIR 1963 SC 1295.
[13]AIR 1950 SC 27.
[14]AIR 1975 SC 1378.
[15]AIR 1995 SC 264.
[16]AIR 1997 SC 568.

 [ISSN 2581-5369]

the Supreme Court extended the ambit of this right and held that individuals had a privacy interest in the content of their telephone communications. In 1990, Chandra Sekhar alleged that the Government was illegally tapping telephones of 27 politicians, including his own. Subsequently, a CBI investigation revealed widespread wiretapping undertaken by the Government. The matter reached the Supreme Court through a PIL filed by the People's Union for Civil Liberties. The Supreme Cout in this case the SC ruled that the Right to Privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution.The right to hold a telephone conversation also comes under the ambit of Right to Life. So, it cannot be curtailed without procedure established by law.

In Justice K.S. Puttaswami v. Union of India[17], the right to privacy was stated by the Honourable Supreme court to be a fundamental right under Article 14, Article 19 and Article 21 of the Indian Constitution. As such, any actions which restrict the right to privacy – such as surveillance – can only be justified through being prescribed by law, which would require the surveillance to be necessary to achieve a legitimate aim and proportionate to that pursued aim. The Supreme Court held that Right to Privacy is a facet of human dignity and so such right is inalienable expect as to procedure established by law.

The Supreme Court laid down the three-fold test in order to test the privacy infirngements. The court moved away from the 'strict scrutiny test' which was being followed in the previous judgements. The court laid down the three fold test, now known as The Puttaswamy three-fold test, which states that in order for legislation to violate the right to privacy, it must fail the following:

1. Legality:

It means that the impugned legislation must not be according to the due process of law.

2. Need:

This means that the restriction laid down by the legislation must be an absolute necessity inorder to achieve the legitimate state aim for the good of general public.

3. Proportionality:

This means that the restriction has a rational nexus with the objects to be achieved, i.e., the legitimate aim of the state. Both the rights must be constructed as harmoniously as possible. The restriction must be proportional to the legitimate goal and not more than that.

There are various other cases including the District Registrar & Collector, Hyderabad v. Canara

[17]AIR 2017 SC 4161.

 [ISSN 2581-5369]

Bank[18], Petronet LNG Ltd v. Indian Petro Group &Anr[19] and Selvi v. State of Karnataka[20]. In these cases, the Supreme Court analyzed the relations between right to privacy and right to life and personal liberty. The court came to a conclusion that the right to privacy is a fundamental right guaranteed by the Constitution of India. The court also decided that a State can intrude upon a person's privacy only in three cases:

- If there is a legislative provision
- By way of administrative or executive order
- By complying with a judicial order.

Thus, through these series of judgements, it is clear that the Right to Privacy is recognized in the Indian Jurisprudence as a fundamental right enshrined under Article 21.

IV. TEST OF PROPORTIONALITY

Since there is very less number of judicial pronouncements available regarding the disputed question of Right to Privacy, it becomes necessary to rely on older principles or doctrines. One such principle is 'Test of Proportionality' evolved from the German Jurisprudence. Usually this test is used by the judges to decide cases where there are two legitimate rights conflicting each other. This test has been applied by the Honourable Supreme Court in the case of Justice K.S. Puttaswami v. UOI[21], inorder to harmoniously interpret the right to privacy of the individual and the right to surveillance of the state.

Generally, this test employs a fourfold mechanism to determine the proportional balance of rights and limitations. These four stages are:

1. Legitimate Goal:

In this stage, the main concern is to check whether the restrictive measure is for a legitimate goal. It is determined whether such a goal is for the good of general public, without any personal grudges against whose right is being restricted.

2. Rational Connection:

The main object of this stage of the test is to study the suitability of the restrictive measure in order to achieve the legitimate goal laid down in the previous stage of the test. In this stage, it must be established that there is a reasonable nexus between the goal to be achieved and the

[18]AIR 2005 SC 186.
[19]5 CS (OS) No. 1102 of 2006.
[20](2010) 7 SCC 263.
[21]*Ibid, at 15.*

 [ISSN 2581-5369]

restriction imposed.

3. Necessity:

After establishing the nexus between the goal and the restriction of the right, it must be established that such a restriction is an absolute necessity, i.e., there must not be any alternative that is less restrictive, but has the same efficiency and effectiveness. It must be clear that the restrictive measure is not an option, but a necessity.

4. Balance:

This is the last stage of test, where the two rights are actually balanced, so that the both the right holders do not have any disproportionate impacts. In this stage, it is to be established that both the rights have been equally balanced in a way that both can be enjoyed harmoniously. This means that the courts must not give preference to a right over another right in a way detrimental to any of the right holder.

This test was used by the Honourable Supreme Court in the case of Justice K.S. Puttaswami v. Union of India, to decide whether the impugned legislation in question was unconstitutional or not. If such a legislation passes all the four stages mentioned above, then it would be regarded as good law and such restriction constitutional.

V. CONCLUSION

After studying both the Right to Privacy and Surveillance by the state through the judicial pronouncements, and the test of proportionality between the both, it becomes clear that both privacy and surveillancemust be harmoniously balanced which is very essential for a welfare state. It would not be correct to say that both privacy and surveillance are against each other, or one must be placed over the other. No welfare state can deny the need of either.

Unless there is an absolute necessity for the state to surveil the actions ofan individual, the state must refrain from doing so. Necessity alone is not enough; unless the state has sufficient evidence of one being involved in a crime, the law enforcement agencies should refrain from intercepting communications of those individuals. The argument saying that the state has an absolute right to intercept all communications and surveil all activities of the citizens for the public welfare can be accepted in a Police State. But in India, now a welfare State, such an argument cannot be encouraged.

At the same time, it cannot be argued that the individual right to privacy overrides the state's power to surveil the activities of an individual. If it so, then a crime can never be prevented; it can only be repaired after the occurrence. So, it is important that both the rights of the

 [ISSN 2581-5369]

individuals and the power of the state must be harmoniously interpreted and the restrictive power must go through a test of proportionality as laid down by the Supreme Court in Justice K.S. Puttaswami v. Union of India.

Coming to the question 'Whether Surveillance is a threat to privacy?' cannot be conclusively decided without considering the actual law in question. It is also important that the government must restrict itself from framing laws that unreasonably restrict the right of privacy of the individual. Thus, the government must frame more efficient and non-intrusive surveillance laws, without excessively disturbing the Right to Personal Liberty.

*****

 [ISSN 2581-5369]