Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

An Analysis of the Pegasus Spyware issue in light of Surveillance Laws and the Right to Privacy in India

Gaurav Kumar[a]

[a]CHRIST University, Delhi NCR, India

Received 18 March 2022; *Accepted* 28 March 2022; *Published* 02 April 2022

Mid of the year 2021 witnessed a global cyber hacking incident by the Israeli cyber-intelligence firm "Pegasus Spyware". The said firm illegally infiltrated the Indian Smart Phones to get the data of several politicians, journalists, judges, lawyers, and businessmen. The said attack directly violated the constitutionally guaranteed fundamental right of 'right to privacy of the citizens. The Government of India is being accused of conducting this snooping. However, the Supreme Court of India has formed an independent committee to probe this issue. The existing surveillance projects like CMS and NETRA have also been accused of collecting bulk data of citizens under the disguise of maintaining public safety. The constitutionality of the said projects has been challenged before the Delhi High Court. Now, the Government's maneuver of giving these projects including Pegasus spyware shield of existing surveillance laws like the Telegraph Act, 1885 and the Information Technology Act, 2000 seems totally unreasonable. The said laws provide target surveillance of telephonic and internet-based communication on identifiable individuals or in the situation of a public safety and emergency issued by the appropriate authority. The constitutional and legal analysis of the bulk surveillance as carried out by Pegasus spyware is long due. In this research paper, we will analyze the constitutionality and legality behind the bulk surveillance carried out under Pegasus and such snooping cases in light of the existing surveillance laws. We will also check the jurisprudential evolution of the right to privacy and how such incidents are violating this right.

Keywords: *Pegasus, right to privacy, surveillance, spyware, constitution, freedom of speech and expression.*

INTRODUCTION

On 18th July 2021, a consortium of 17 journalist organizations around the world including one Indian organization made global headlines and sparked political controversies by revealing the alleged fact that an Israeli cyber-Intelligence firm NSO group's Spyware targeted 50,000 mobile phones for hacking to get personal data. According to the said report, more than 300 Indian mobile phones have been targeted by the Israeli spyware, including two of the serving central ministers of the Union Cabinet, three opposition leaders, sitting judges, politicians, several journalists, lawyers, human-right activists, and business persons. The report indicates the Pegasus spyware firm illegitimately and unlawfully infiltrated the Indian smartphones to get access to the entire data of smartphones and they sell the same to government officials. However, *the central government denied all the facts and said that the report is "sensational" and seems to be an attempt "to malign Indian democracy and its well-established institutions". The NSO group also claimed that the "allegations of snooping were false and misleading".*[1]Recently, an investigation conducted by New York Times reported that the Indian Government had purchased the Israeli NSO group's Pegasus software[2] for carrying out surveillance on the targeted citizens. This news gathered uproar from the opposition as the state can't infringe the constitutional rights of the citizens. A batch of petitions was filed in the Supreme Court seeking a fair investigation into the Spyware scandal by SIT under the mentorship of the Court itself. The petitioners claimed that it is a matter of serious concern because the government is endorsing the Pegasus spyware for the cyber-attack on Indian citizens that has directly violated the right to privacy. The three judges bench has appointed an "Expert Committee" presided by Justice (Retd.) R V Raveendran to inquire into the Pegasus scandal. During the investigation, the members of the technical committee found strong indicators which pointed out the role of the state, its intelligence, and law enforcement agencies in using Pegasus

[1] 'A timing of the Pegasus Snooping Scandal' (*The Indian Express*, 27 October 2021) <https://indianexpress.com/article/india/a-timeline-of-the-pegasus-snooping-scandal/> accessed 08 March 2022

[2] 'Opposition Slams Government as New York Times says India brought Pegasus spyware' (*The Hindu*, 29 January 2022) <https://www.thehindu.com/news/national/pegasus-and-a-missile-system-were-centerpieces-of-2-billion-deal-between-india-and-israel-in-2017-nyt/article65013909.ece> accessed 08 March 2022

spyware against the citizens[3]. The members found the specific IP addresses during their forensic analysis which are only reserved by the networks for their corporate clients including the Government of India. The current analysis conducted by the SC Committee points out the involvement of the State and the Law enforcement agencies against the Citizens of India. The research paper shall critically analyze the issue of cyber attacking in light of the legal as well as the constitutional position of the right to privacy.

WHAT IS PEGASUS?

It is a spyware firm developed by an Israel-based Cyber- Security Company named NSO group. It is a kind of malicious software that hacks into smartphones to collect the stored data and sell the same to third parties without the consent of the concerned parties. The malware becomes activated when it enters the phone and gets all access to keep track of the activity of the phone including contact list, SMS, gallery, files, and location. The said software can also strike on encrypted chat, audio, and videos.

LAWS RELATED TO SURVEILLANCE IN INDIA

The laws prevailing in India related to surveillance are:-

1. Article 19(2) of the Constitution of India allows *the government to impose reasonable restrictions on freedom of speech and expression in the interest of or State Government in the interests of sovereignty, and integrity of India, the security of the state, friendly relations with foreign state or public order, decency or morality or in relation of contempt of court, defamation, or incitement of an offense.*[4]

So, in case the government feels that there is a threat to the security and integrity of the nation, it can restrict the freedom of speech and expression of the Citizen.

2. The Indian Telegraph Act, 1885 (IT Act, 1885)

[3] Ashish Aryan, 'Digital Trail points to Pegasus, state role: expert told SC panel' (*The Indian Express*, 1 February 2022) <https://indianexpress.com/article/india/digital-trail-points-to-pegasus-state-role-experts-told-sc-panel-7750425/> accessed 08 March 2022

[4] Constitution of India, 1950, art. 19(2)

In case of occurrence of public emergency or in the interest of public safety, Section 5 (2) of the Indian Telegraph Act, 1885 allows the lawful interception by the Central Government, State Government, or any specially authorised officer of Central Government or State Government in the interests of sovereignty, and integrity of India, the security of the state, friendly relations with foreign State or public order, or for the preventing incitement to the commission of an offence.[5] However, a proviso to Section 5(2) of the said Act states that such lawful interception can't take place against the Journalists. In the case of ***Public Union for Civil Liberties v Union of India***[6] when the Supreme Court was dealing with the issue pertaining to infringement of 'Right to Privacy', it confirmed that the tapping of telephonic conversation violated the 'Right to Privacy'. The Court laid down some procedural safeguards against the arbitrary surveillance power used by the State and its agencies. The PUCL guidelines focused on upholding the right to privacy against State Surveillance and shaped a path for the protection of the right to privacy in the future era of the 'Digital Age'. At a later stage, the PUCL guidelines were specified by inserting Rule 419A[7] in the Indian Telegraph Rules, 1951 through its 2007 amendment. The rules included that the orders on the interception of communications shall be issued by the Secretary in the Ministry of Home Affairs of the Central Government or the State Government. However, the rules were not followed in a serious manner, and the telephonic tapping and leakage of Call Data Records incidents of the politicians by the private agencies and police officers were usual. In 2012, the changed Government of Himachal Pradesh disclosed[8] that 1371 telephones were targeted for surveillance by the previous government where only 2 percent of them were authorised by the Home Secretary.

3. The Information Technology Act, 2000 (IT Act, 2000)

Section 69 of the Information Technology Act, 2000 provides power to the competent authority for the interception or monitoring, or decryption of any information through any computer

[5]Indian Telegraph Act, 1885, s 5(2)
[6] *People's Union of Civil Liberties v Union of India* AIR 1997 SC 568
[7] Indian Telegraph Rules, 1951, r 419-A
[8]Pranesh Prakash, Misuse of Surveillance Powers in India (Case 1)' (*The Centre for Internet and Society,* 6 December 2013) <http://cis-india.org/internet-governance/blog/misuse-surveillance-powers-india-case1> accessed 18 February 2022

resource in the interest of sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence. [9] However, the said provision is subject to sub-section (2) of Section 69 of IT, Act 2000 which establishes the procedures and safeguards for lawful interception by the competent authorities. The rules under the IT (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 provide that the competent authority can order the interception, decryption, or monitoring of any information stored, generated, or transmitted in any computer resource. The competent authority under the said rules is the Secretary in the Ministry of Home Affairs. In December 2018, the Central government under the IT rules, 2009 authorised 10 central agencies namely the Intelligence Bureau, the Central Bureau of Investigation, the National Investigation Agency, the Research & Analysis Wing, the Directorate of Signal Intelligence, the Narcotics Control Bureau, the Enforcement Directorate, the Central Board of Direct Taxes, the Directorate of Revenue Intelligence and the Delhi Police Commissioner to conduct surveillance. Under Rule 4 of the IT Rules, 2009 the above mentioned central agencies may intercept, monitor, or decrypt the information received, stored, or generated in any computer resource. The said action of the government was criticized and challenged in the Supreme Court. Unlike the Telegraph Act, 1885, the exclusion of the provision of "occurrence of public emergency or in the interest of public safety" from the IT Act, 2000 provides wide scope to the government for the interception of any information.

SURVEILLANCE PROJECTS IN INDIA

Post Mumbai Terror attacks in the year 2008, the Government of India implemented several policies pertaining to surveillance. The surveillance projects were implemented to increase public safety and counter-terrorism and crime. The National Intelligence Grid (NATGRID), Crime and Criminal Tracking Network and Systems (CCTNS), Lawful Intercept and Monitoring (LIN), Network Traffic Analysing System (NETRA), Central Monitoring System,

[9] Information Technology Act, 2000, s 69

and various other state monitoring systems were implemented in order to enhance the public safety. However, the projects have faced having an accusation of putting the citizens on 360-degree surveillance by collecting data. The said projects can monitor a person's phone conversation, and track GPS location which is a violation of the right to privacy under Article 21 of the Constitution of India. A PIL filed by the Centre for Public Interest Litigation (CPIL) and Software Freedom Law Centre (SFLC) contended that the surveillance projects of the governments allow intercepting and monitoring of all kinds of telecommunications which is ultimately a contravention to the Puttaswamy Judgement. The Court asked the Centre to file a detailed reply in this regard as the next date of hearing is on March 23, 2022.

Now, the pertinent question in this regard is *whether Section 5(2) of the Telegraph Act is applicable in all kinds of bulk surveillance conducted by the Government under surveillance projects?*

Section 5(2) of the Telegraph Act, 1885 reads-

"*On the occurrence of any* ***public emergency****, or in the interest of* ***public safety****, the Central Government or a State Government or any Officer specially authorised on this behalf by the Central Govt. or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of and offence, for reasons to be recorded in writing, by order, direct that any message clear of messages to or from any* ***person or classes of persons****, relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detailed, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order*"

The answer is no as the said provision intends to intercept the telegraphic messages of an individual for a specific short period. Secondly, the term '*persons or class of persons*' in Section 5(2) denotes specifically identifiable individuals and not the whole citizenry, and last the interception shall be done either on the occurrence of '*public emergency*' or in the interest of '*public safety*. So, the said provision neither allows bulk surveillance of the citizenry as a whole nor authorizes the surveillance projects to do.

Now, *whether the second provision of Section 69 of the Information Technology Act, 2000 and rules under The Information Technology (Procedure and Safeguards for Interception, Monitoring, and decryption of information) rules, 2009 is applicable on the issue of "bulk surveillance"*?

The answer is no as in the aforementioned provisions the interception or monitoring of the computer devices shall be only done after the order of the competent authority, not below the rank of Joint Secretary of the Ministry of Home Affairs in the central or State Government. However, in case of an **emergency** where due to operational reasons the prior instructions are not available and the area is **remote,** the monitoring or interception shall be done by the second most officer, not below the rank of Inspector General of the law enforcement agency at the central or state level. So, the said provisions only allow intercepting or monitoring a specific source for a particular duration instead of collecting the data of citizens a masse. Let's assume that the provision allows the surveillance project to collect the data of citizens under the blanket protection of interception even that will require the order of the competent authority (as provided under the act). Despite judicial pronouncement of the right to privacy as an intrinsic part of Article 21, the Government has been jeopardizing the privacy of the citizens under the blanket of executive orders without providing any legislative backup to its surveillance projects. These issues are pending before the Hon'ble Delhi High Court in the case of ***CPIL and ANR vs Union of India[10].***

RIGHT TO PRIVACY

International Position

Article 12 of the Universal Declaration of Human Rights, 1948 provides *that no one shall be subjected to arbitrary interference with his privacy, family, and home, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interferences or attacks.*[11] According to Article 17 of ICCPR, 1966 *"a person's privacy, home, family or correspondence should not be subjected to any arbitrary intrusion nor his honor and reputation".*[12]India ratified it on 11

[10] *CPIL and Anr v Union of India* (2020) Writ Petition (Civil) No. 8998
[11] Universal Declaration of Human Rights, 1948, art. 12
[12] International Covenant on Civil and Political Rights, 1966, art. 17

December 1977. The report of the UN High Commissioner for Human Rights on June 30, 2014, said that " there is a universal recognition of the fundamental importance and enduring relevance of the rights to privacy and of the need to ensure that it is protected in law and in practice[13]" Article 8 of the European Convention on Human Rights states "*Everyone has right to protect his private and family life his home and correspondence.*"

Indian Position

The Right to Privacy is not mentioned in the Constitution of India. However, it is now a part of Article 21 of the Indian Constitution through judicial interpretation. Earlier, the position of the Supreme Court in the case of ***MP Sharma v Satish Chandra***[14]and ***Kharak Singh v State of UP***[15] was that Privacy is not a fundamental right and there is no constitutional protection for the same. In the case of ***People for Civil Liberties v Union of India,***[16] the Supreme Court held the taping of telephonic conversation of an individual in the home or office which is in private nature shall be amount to a violation of the right to privacy. The apex court ruled that interception can be allowed only in the interest of public safety or on the occurrence of any public emergency. In this case, the Hon'ble Court had issued certain guidelines for the interception so that a fair procedural safeguard ought to be adopted by the government during interception. On 24th August 2017, the 9 judges-bench of the Supreme Court delivered a historic decision in the case of ***Justice K. Puttaswamy (Retd.) &Anr. v Union of India*** [17]held that the Right to privacy is a fundamental right, which is an integral and intrinsic part of the right to life under Article 21 of the Constitution. Therefore, it is now a constitutionally protected right therefore, in case of violation of the right to privacy, the writ application can be filed in the constitutional court for seeking a remedy. However, the Apex court said that like other fundamental rights, the right to privacy is not an absolute right and it is subject to

[13] Dr. Keith Goldstein, Dr. Ohad Shem Tov, & Mr. Dan Prazeres, 'The Right to privacy in the Digital age' (*United Nations High Commissioner for Human Rights*, 9 April 2018) <https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf> accessed 10 March 2022

[14] *MP Sharma v Satish Chandra* (1954) 1 SCR 1077

[15] *Kharak Singh v State of UP* (1963), AIR 1295

[16] *People's for Civil Liberties v Union of India* (1997) 1 SCC 301

[17] *Justice K. Puttaswamy (Retd.) & Anr. v Union of India* (2017) 10 SCC 1

reasonable restrictions. That doesn't mean the state can encroach on the right to privacy illegitimately and without proper cause. The court directed that there must be a balance between individual interest and legitimate state interest. That means when the state is going to encroach on the right to privacy, there must be in accordance with the constitutional mandate otherwise the encroachment shall be invalid or unconstitutional. For this purpose, the court said that the encroachment of the right to privacy by the state shall have to withstand three-fold tests which are:-

- **Legality -** the action must be sanctioned by law;
- **Necessity -** there must be a need for that action for the legitimate aim;
- **Proportionality –** there must be proportionate action that ensures rational nexus between the objects and means adopted to achieve them.

Therefore, it must be ensured by the state while curtailing the right to privacy that is according to the constitutional need and three-fold tests. When the state's action is disproportionate without legitimate aim, it shall be invalid and unconstitutional. In ***Anuradha Bhasin v Union of India***[18], the validity of the shutdown of Internet and movement restrictions was challenged in this case, while deciding the case the Supreme Court held that the competent authority must take the doctrine of proportionality into consideration during the time of imposing restrictions on fundamental rights.

CURRENT POSITION

There is no specific law for the protection of data privacy in India. In ***Puttaswamy Case I,***[19]the Supreme Court constituted a committee under the headship of Justice B.N. Krishna for preparing a draft on the "Data Protection Framework". The committee submitted a report on the same to the Government of India. The Data Protection Bill, 2019, is still pending in

[18] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637
[19] Justice K. Puttaswamy (Retd.) (n 17)

Parliament to enact. The said bill provides a robust mechanism to deal with matters relating to data privacy and its protection.

INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011

The Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 is one of the existing data protection laws which has been framed under Section 43A[20] of the Information Technology Act, 2000. The provision was inserted by Information Technology (Amendment) Act, 2008[21] which was enacted on October 27, 2009. The aim of the section was to provide rules of practice and procedures followed by the body corporates that pass and handle any sensitive data. Section 72A[22] of the IT Act, 2000 is a penal provision in case of an intentional data breach and compensation to be provided against such intentional breach. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 was enacted pursuant to the intent of Section 43A of the IT Act, 2000.

The objective of the 2011 rules is to deal with sensitive personal data or information stored in a computer resource under the ownership of a body corporate. The rules are made to deal with specific sensitive data like passwords, financial information, biometric information, medical records, sexual orientation, etc., and not non-sensitive data. The rules have a certain limitation as it applies only to the body corporate like firms, proprietors, or group of individuals who are engaged in professional or commercial activities. So the individuals and Non-Profitable Organisations shall fall outside the ambit of "body corporate" as defined under the act. The second limitation is that the rules are only meant to deal with electronic data. So, data that is not in electronic form shall fall beyond the ambit of 2011 rules.

[20] Information Technology Act, 2000, s 43A
[21] Information Technology (Amendment) Act, 2008
[22] Information Technology Act, 2000, s 72A

OTHER LAWS

Indian Penal Code, 1860[23] also deals with penal provisions in case of data breach or theft. Section 403[24] deals with dishonest misappropriation or conversion of movable property. The said section specifically doesn't provide data as movable property but still in case of data theft the case can be registered. Credit Information Companies (Regulation) Act, 2005[25] deals with the protection of the banking data of the consumers. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 framed under Section 87(2)[26] of the Information Technology Act, 2000 deals with the due diligence followed by the data intermediary (including social media intermediary). On July 22, 2021, a petition was filed in the Supreme Court in the case of ***Manohar Lal Sharma v Union of India,***[27]for seeking a fair and impartial investigation by SIT under the court itself into the Pegasus spyware data scandal and it was also sought for the prosecution of the accused who are involved in buying or snooping of data of Indian Citizen by Pegasus spyware. The Court was directed to the Central Government to provide the details regarding the Pegasus Spyware. However, the government declined to reveal the details of facts before the Supreme Court on the grounds of national security concerns. The Court said that it is very well-settled that the scope of judicial review is very limited in matters of national interests; it doesn't mean the government would get blanket immunity from the scrutiny of judicial review by citing the concern of national security. The Court observed that it is a violation of the right to privacy when surveillance or snooping is done on the citizen either by the State or by any external agency. However, if the same is done by the state then it must be in accordance with the constitutional mandate. The Court relied on the proposition laid down by the Supreme Court in the case of ***Justice K. Puttaswamy I***[28]that the right to privacy is a fundamental right and it is a part of Article 21. The Supreme Court observed that the information gathered by surveillance through the intelligence agency must be for a reasonable purpose. To access the information of an individual, there must be the

[23] Indian Penal Code, 1860
[24] Indian Penal Code, 1860, s 403
[25] Credit Information Companies (Regulation) Act, 2005
[26]Information Technology Act, 2000, s 87(2)
[27] *Manohar Lal Sharma v Union of India* (2021) SCC Online SC 985
[28] *Ibid*

necessary information for combating crime or terror in the national interest. The Court has directed to appoint of three members expert committee that will look into the Pegasus spyware Case and they will reveal the truth regarding the large scale violation of fundamental rights.

ANALYSIS

M.P Sharma vs Satish Chandra[29] was the first case where the Supreme Court threw light on the right to privacy. The question in issue was whether the Right to Property under Article 19(1)(f) of the Constitution is violated by the search and seizure conducted by the state agencies. The courts uphold the 'search and seizure' as the state holds overriding power for the protection of social security and it is regulated by the law. Simultaneously, the court recognized the 'right to privacy with a comment that when the constitutional makers didn't put it within the constitutional limitations, it had no justification to put it within the realm of another fundamental right by the process of strained construction. So, at that time the constitutional courts tried to stick with the bare provisions of the constitution and prevented it from expanding its ambit.

The year 1963 witnessed a new paradigm in the 'right to privacy when U.P Police Regulations were challenged in the case of ***Kharak Singh v State of U.P***[30]**.** The said regulation vested unfettered surveillance powers to the State upon the '*history sheeters*'. The regulations were challenged on the ground as they violated freedom of movement under Article 19(1)(d) and personal liberty under Article 21. The preliminary observation is whether the restriction under Articles 19(2) and 19(6) was applicable to the administrative regulation as it doesn't form any law. The defense under Article 19(2), 19(6), and Article 21 (*procedure established by law*) is only available against the law made by the state and not the administrative regulations. The court found that the regulations put restrictions only on those individuals who were suspected to have indulged in proven antisocial activities and it was necessary to put a reasonable restriction for the protection of society. The court agreed that the classification was reasonable

[29] MP Sharma (n 14)
[30] Kharak Singh (n 15)

and it aimed to preserve public order. The Court held that the "*right to privacy is not a part of our constitution and mere putting a reasonable restriction over the citizen's movement doesn't violate fundamental rights enshrined under part III of the constitution*". Again, in this case, the court touched the brink of 'the *right to privacy* but it denied it to give recognition under the Constitution under Part III.

A partly dissenting judgment given by Justice Subba Rao, in this case, stated that *'although the* ***right to privacy*** *is not expressly provided in the constitution as a fundamental right the said right is an essential part of* ***personal liberty.*** He further defined privacy as a right 'to be free from every restriction or encroachment on a person whether it is imposed directly or indirectly by the calculated measure'. The dissenting opinion was noted in Puttaswamy Judgment (Aadhar case) and the right to privacy was recognized as an intrinsic part of "*fundamental rights*" under Article 21 of the Constitution. The year 1975 brought a historical moment for 'privacy law' in the Indian Constitution. In the case of ***Govind vs State of M.P***[31] like in the *Kharak Singh case*, a Regulation that involved a domiciliary visit to the house of the history-sheeter was challenged on the ground of violation of Articles 19 and 21. However, in this case, the court found that the regulation had statutory backing which allowed the state to make notifications giving effect to the provision of the statute in order to prevent the commission of the offence. The court found that the regulations specifically intended to prevent the "history-sheeters" repeating offenders, from the commission of the offense. This was the moment when dissenting judgment by Justice Subba Rao in the Kharak Singh case was taken into consideration who had stated that domiciliary visits violated free movement (Article 19{1}{d}) as well as individuality under Article 21. The court in the case cited the U.S Supreme Court judgment of *Griswold v Connecticut (381 U.S. 479)* and observed that the law infringing the right to privacy must satisfy the '***compelling state interest test***'. The Court in this case held that even if freedom under Article 19 and Article 21 gave rise to a distinct fundamental right to privacy, which is not absolute in nature and is subject to the "***compelling state interest test***" as under Article 19(5). The court also cited Article 8 of the European Convention on Human Rights, which recognized the right to privacy but it puts a reasonable restriction on its enjoyment. The court added that a

[31] *Govind v State of M.P* (1975) 2 SCC 14

domiciliary visit won't automatically amount to an unreasonable restriction on privacy. If it is presumed that the right to privacy is an integral part of Article 21, then it can be curtailed only by the '**procedure established by law'.** The court in this case applied a narrow interpretation to the regulation in order to save it from unconstitutionality giving it the backing of Article 19(5) of the constitution of India. The regulations were narrowly interpreted in a way that included a particular class of citizens who had a background of repeated offenders and excluded the law-abiding ones. The Gobind case for the first time showed a ray of incorporating the 'right to privacy in the Indian Constitution and paved a way for the constitutional courts to move ahead with interpreting the ambit of Article 21. Now, the bulk surveillance projects of CMS, and NETRA which are violating the right to privacy of citizenry would put pressure on the State to demonstrate how the collection of every data is necessary for public security.

The year 1997 turned out to be an important one in the era of the '*right to privacy*. In the case of ***People's Union for Civil Liberties (PUCL) v Union of India***[32] where Section 5(2) of the Telegraph Act, 1885 was challenged during the inquiry of the telephone tapping. The telephone tapping was held to be a violation of the right to privacy. However, the court applied narrow tailoring of the provision instead of declaring it unconstitutional. The court in this case interpreted the phrases '*public safety* and '*public emergency*'. The Court held that the two phrases 'take their color off each other'. It defined public safety as a state of safety or freedom from danger to the public at large and argued that neither a public safety nor public emergency can be secretive, nor must be evident to the reasonable person. The court said that two conditions (public safety and public emergency) are prerequisites for exercising the power to intercept and provided guidelines in form of safeguards to check the arbitrariness in terms of issuing surveillance orders. These guidelines were later codified under Rule 419A of the Telegraph Rules, 1951. So, the *PUCL case* became a landmark case where the court had evolved the jurisprudence of '*public safety and public emergency*' as a prerequisite for interception by state agencies. The key takeaway from PUCL is as-

[32] People's Union of Civil Liberties (n 6)

- The Telegraph Act specifically intends to provide targeted surveillance. Neither the court nor the act contemplates bulk surveillance as what happened in the Pegasus case.

- The Court denied judicial review in targeted surveillance. It doesn't mean that it is not even required in bulk surveillance like Pegasus.

- *PUCL guidelines* were required to be followed in targeted surveillance which was later codified into Rule 419A of the Telegraph Rules, 1951.

- The Privacy restrictions must be narrowly tailored (if they are constitutional) and target s specific suspicion on identifiable individuals and are only meant to fulfill the public safety and crime prevention goal of an Individual.

The court in *PUCL* added a narrow tailoring test after a compelling state interest test given in *Govind* for the infringement of privacy. Now, the common point in these cases was the "target surveillance" of either specifically identifiable individuals who were in suspicion of being repeated offenders or an individual whose privacy was breached due to phone tapping. The Court's approach in identifying the right to privacy and balancing the surveillance powers of the state was in light of the reasonable classification which separated 'a specific class' from a normal mass. *Will this approach stay fit in Pegasus Spyware and Surveillance projects like CNS and NETRA where bulk surveillance is carried out by the State in the disguise of achieving public safety?* The year 2017, ten years post-PUCL saw a historical move of the Supreme Court in the case of ***Justice K.S Puttaswamy vs Union of India***, where the Supreme Court was revisiting the issue that whether 'right to privacy is an integral component of fundamental rights under Part III of the Constitution? The Court found that the right to privacy is an inalienable and natural right and it is related to human dignity. The said right is not independent of other freedoms guaranteed by the constitution under Part III. However, this right is not an absolute one and can be encroached on by competing for state and individual interests. The court in this case held that 'the right to privacy as an intrinsic part of Article 21 can be denied only through "**procedure established by law**" which must be '*just, fair and reasonable.* The court provided a threefold test that is required to be withstanding by the State in case of a right to privacy

encroachment. So, do we consider that the bulk surveillance by 'Pegasus spyware' is in consonance with the three-fold proportionality test provided in*Puttaswamy*? The past year 2021 witnessed a ruckus over the right to privacy issue when the cell phones of politicians and journalists were hacked by 'Pegasus' an Israeli spyware software. The petitioners moved to Supreme Court against such data breach as it was alleged that the said hacking was carried out on the order of Govt. of India. The court formed a committee to probe this mass privacy violation case

In ***Manohar Lal Sharma v Union of India***[33]**,** most commonly known as Pegasus Spyware Probe, the Supreme Court has rightly pointed out that there must be a balance between the fundamental rights of an individual and national security. The state cannot take away the fundamental right of an individual by merely citing the cause of national interest. The State has to pass three-fold tests of proportionality which have been laid down in the ***Puttaswamy I case***.[34] If the state is encroaching on the right to privacy of individuals by snooping or surveillance then it must be in accordance with legitimate law for the reasonable purpose in the national interest.

CONCLUSION

From M.P Sharma to Puttaswamy, it took a span of almost 60 years to evolve the jurisprudence of '*right to privacy* in the Indian Constitution. The Court adopted different approaches to testify to the reasonability of state interception in an individual's personal life. In the diversity of cases, we have analyzed the scope of the right to privacy embedded in our constitution and under what grounds the state's interception of one's privacy is reasonable. From the compelling state interest test, public safety, and emergency test to the three-fold proportionality test the courts have laid down that the law restricting privacy must be tailored narrowly. In simple words, the state must show that the infringing law not only achieves the compelling state interest but it also restricts the right to privacy in the narrowest possible manner. If a similar goal can be achieved in other ways rather than infringing the privacy that

[33] Manohar Lal Sharma (n 27)
[34] Justice K. Puttaswamy (Retd.) (n 17)

the impugned law does, the said law shall be struck down. In Gobind, the regulation in question was narrowly tailored instead of striking it down because the State had no other option to shift except infringe privacy at the minimum. However, the surveillance projects and Pegasus Spyware include bulk surveillance by the state (if it is proved) over the law-abiding citizenry. There is no legislative backing or the 'compelling state interest' that needs to be achieved nor does it shows to abide by the three-fold proportionality test. Now, there is a burden on the Court to readdress the issue of mass privacy violations through spy incidents of cell phone hacking as with the improvement of technology there is a fear of getting sensitive data of the individual jeopardized. On the contrary, the State has to prove how its bulk surveillance projects are necessary to uphold public safety and for such purpose, the breach of privacy of Individuals is in consonance with the three-fold proportionality tests laid down by the Court in Puttaswamy.

The Constitution of India doesn't just provide the fundamental right to an individual but it also protects and guarantees the same. It ensures that the state cannot take away an individual's right without proper reason and fair manners. Therefore, if the state encroaches on those fundamental rights (i.e. the right to privacy) then it must be ensured that the same is done by the legitimate law with the legitimate aim in a proportional manner for the public interest otherwise that kind of action must be invalidated by the constitutional court. It is the constitutional duty of the state to protect the citizen's fundamental rights. For that purpose, the government must enact the law on data privacy and its protection very soon so that this kind of unfettered action of government can be checked with effective and clear law. We hope that this time the court shall apply a new approach and protect the privacy of the citizenry.