
THE IMPACT OF THE RECENT PEGASUS SPYWARE CONTROVERSY ON THE RIGHTS TO PRIVACY IN INDIA

***WASIM RAZA**

ABSTRACT

An Israeli organization called NSO developed Pegasus spyware with the goal of assisting governments around the world with monitoring, mostly to eradicate wrongdoings there. Contrary to its stated objectives, Pegasus spyware is not employed to stop such acts; rather, its use has led to the violation of several people's right to privacy. For instance, it is said that the mobile phone of Mr. Rahul Gandhi, the leader of the Congress party, was assaulted using the Pegasus spyware to investigate the tactics used by opposition parties. Nearly 1,000 of the 50,000 well-known individuals who could be targeted by this spyware, according to a report released by Amnesty International, are Indian citizens. The Pegasus spyware is a platform for destroying the cornerstone of democracy, eliminating the independence of the court, and repressing those who seek to expose the wrongdoing of those in positions of authority. The Supreme Court reached a well-respected ruling in case of Justice K.S. Puttaswamy v. Union of India, paving the way for the right to be enshrined into the Indian Constitution. Several laws connected to monitoring have also been broken as a result of the Pegasus malware. Additionally, the Pegasus malware has led to violations of several laws pertaining to monitoring. However, it is important to note that the Union Government has deemed the accusations of such surveillance as "baseless, fake, and concocted" and has expressed reluctance to accept any such charge.

Keywords: - Right to privacy, spying, Pegasus, democracy.

*PH.D., UNIVERSITY COLLEGE OF LAW, MOHANLAL SUKHADIA UNIVERSITY, UDAIPUR, RAJASTHAN

INTRODUCTION

The inclusion of the right to privacy in Article 21 of the Indian Constitution is one of the most important developments in independent India's history. For a sizable portion of India's history as an independent nation. One of the notable Janta Party leaders, Mr. Morarji Desai, the fourth prime minister of independent India, highlighted the right to privacy in one of the few cases. Several opposition politicians, journalists, activists, etc. were detained as a result of the emergency declaration by the Indira Gandhi administration in 1975. Mr. Morarji Desai was one such leader. After the declaration of a state of emergency was lifted, a huge group of media arrived outside Mr. Morarji Desai's home, where he declared, "This is a violation of my right to privacy." The phrase "right to privacy" was first used in this situation.

India, however, came into the debate over the right to privacy a little bit later than other nations. Given the circumstances, the 2017 ruling in Justice *K.S. Puttaswamy V. Union of India*¹ protected the right to privacy as a basic right in the Indian constitution. The nine-judge panel unanimously found that the Indian Constitution's articles 14, 19, and 21 protect the right to privacy as a basic freedom. The "Pegasus (spyware)" spyware has recently compromised people's right to privacy. NSO, an Israeli organization, is the maker of Pegasus. Since the Pegasus spyware infiltrates the target person's mobile device and extracts information like images, videos, conversations, notes, passwords, record videos, track GPS, etc. and grants access to such data to other people, this claim that it is one of the most dangerous cybersecurity attacks is by far accurate. Both the widely used operating systems, Android, and iOS, are targeted by the spyware. The severity of the spyware is such that Emanuel Macron, the president of France, changed his mobile phone when the outbreak was reported and after learning that he was one of the Pegasus spyware's prospective targets. According to the NSO organization, the spyware was developed to:

1. Defeat and prevent terrorism
2. Fighting sexual assault and stopping the trafficking of illegal drugs
3. Locate and save kidnapped kids
4. Support emergency search and rescue efforts².

¹ Justice K.S. Puttaswamy V. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

² Use cases, NSO GROUP, available at <https://www.nsogroup.com/about-us/>, last seen on 07/05/2023

The key concern is how this spyware gets into electronic gadgets, so how does it do that? When iOS devices were involved, this spyware used to join by clicking on specific links and URLs delivered via WhatsApp, SMS, and Message. Even said, spyware has become so much more modernized and sophisticated that it can now access your system with just a single missed call on a mobile phone³. The identities of the majority of the 50,000 people on a leaked list of people who are reportedly Pegasus spyware targets or potential targets are those of politicians, journalists, media outlets,⁴etc. The objectives of Pegasus spyware, as stated on the NSO website, do not justify the names of the individuals, who include academics, journalists, lawyers, and leaders of opposing political parties. According to the Central Intelligence Agency, a journalist named Jamal Khashoggi was murdered in 2018 at the king of Saudi Arabia's alleged request. Jamal Khashoggi, a Saudi journalist, was allegedly murdered by the Saudi government recently, and an investigation revealed that the journalist's wife's mobile phone had the Pegasus spyware planted on it months before to the killing.⁵ Listed among the known Indian names in Pegasus spyware are:

1. Rahul Gandhi -Former Member of the Lok Sabha
2. Prashant Kishor - a political operative
3. Ashok Lavasa- Former election commissioner of India
4. Umar Khalid -- Former president of Jawaharlal Nehru University's Democratic Students Union
5. Rakesh Asthana- Police Commissioner of Delhi
6. Anil Ambani- Businessman

³ Etch Explainer: What is Pegasus spyware and how it works - The Economic Times (indiatimes.com) last seen on 07/05/2023

⁴ Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, available at <https://www.amnesty.org/en/latest/news/2021/07/the-Pegasus-project/>, last seen on 07/05/2023.

⁵Revealed: murdered journalist's number selected by Mexican NSO client | Mexico | The Guardian last seen on 07/05/2023

As a result, the Pegasus spyware raises concerns about the spirit of democracy and the proper use of authority. Even more surprising is the report's assertion that the Pegasus spyware specifically targeted two Supreme Court of India staff, lawyers, and even a sitting judge.

HIGHLIGHTS OF THE SUPREME COURT OBSERVATIONS ON SURVEILLANCE:

➤ ***Public Union for Civil Liberties v Union of India (1996)***⁶

- In this case the Supreme Court laid down certain guidelines for interceptions.
- The CBI report on “Tapping of Politicians’ Phones” prompted the filing of a public interest lawsuit.
- The court remarked that the authorities intercepting communications were not even keeping proper documentation and records of their interceptions.
- The court noted that tapping constitutes a serious violation of a person's privacy. The freedom to conduct telephone conversations in the solitude of one's home or place of business without interruption is increasingly abuse-prone as highly sophisticated communication technology develops.
- Therefore, the court ruled, the right of citizens to privacy must be preserved from abuse by the current government.
- One of the guidelines the court set was the creation of a review committee with the authority to look into authorizations received in accordance with Section 5 (2) of the Telegraph Act.

➤ ***R Rajgopal alias RR Gopal and another Vs State of Tamil Nadu (1994)***⁷

- According to the Supreme Court, Article 21's applied on all inhabitants of this nation includes an implicit right to privacy.

➤ ***SUPREME COURT JUDGMENT IN JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA***⁸

- The court's disagreement over the existence regarding the right to privacy was, resolved when a bench of nine judges ruled that it is a basic right.
- The court later stated that the State's use of personal data obtained through telephone and internet hacking falls under the category of privacy.

⁶ AIR 1997 SC 568,

⁷ 1995 AIR 264,

⁸ WRIT PETITION (CIVIL) NO. 494 OF 2012

- In accordance with Rule 419A, the Ministry of Home Affairs' and the secretary-level officer respectively, may issue interception orders for the federal government and the state governments, respectively.
- One of the changes that will be recorded in the annals of Indian history is the Aadhar judgement, which saw the Supreme Court reemerge as the defender of Indian citizens. The decision is historic in and of itself, because it served as the basis for two more historical judgements that further ensured citizenship equality and enhanced freedom, it gains far more significance. The judgements are detailed below.: -
 - i. ***navtej singh johar v. union of india***⁹- In India, this Supreme Court decision decriminalized any adult consensual intercourse, including homosexual sex.
 - ii. ***joseph shine v. union of india***¹⁰ - In addition, this Supreme Court judgement decriminalized adultery, removed a dated section of the Indian Penal Code, 1860, and abolished section 497 of the Indian Penal Constitution.
- The Aadhar judgement is the more well-known name for the ruling. The constitutional legitimacy of Aadhar was contested in a petition by retired court Justice K.S. Puttaswamy because it infringes the right to privacy.
- According to the petitioner in this case, violating the right to privacy, would arise from requiring the use of Aadhar, which is a fundamental element of the right to life and personal liberty under article 21 of the Indian constitution. Mandating the use of Aadhar will result in a fundamental violation of the right to life and personal liberty guaranteed by article 21 of the Indian constitution.
- The government responded by claiming that the constitution nowhere assures citizens of their right to personal privacy. Additionally, the respondent's contention was that the Aadhar act of 2016 only required certain personal information from Indian residents to maintain proper government surveillance.
 - The petitioner's arguments were upheld by the nine-judge constitutional court, which also recognized the right to privacy protected by Indian Constitution. The decision was made to consider the right to privacy a fundamental and important right. Additionally, the 57 and 33(2) provisions of the 2016 Aadhar Act were abolished.

⁹ (2018) 10 SCC 1

¹⁰ 2018 SCC Online SC 1676

➤ ***Manohar Lal Sharma Vs Union of India:***¹¹

The three-judge bench of supreme court ordered a probe into the Pegasus controversy¹². The retired judge's probe into the spyware, Pegasus, will be supported by the court's appointment of an impartial expert committee.

➤ **Technical committee** –On Wednesday, the Supreme Court of India established an expert committee to look into the Pegasus snooping scandal, which it claimed had jeopardized the privacy of both persons and institutions. The three-member committee will be led by retired Supreme Court justice RV Raveendran, according to a bench consisting of Chief Justice N V Ramana, Justices Surya Kant, and Hima Kohli. The Centre has refused to submit a thorough affidavit in the case, citing national security.¹³.

Technical committee has been established constituting three experts namely -

- I. **Dr. Naveen Kumar Chaudhary**, Professor (Cyber Security and Digital Forensics)
- II. **Dr. Prabakaran P.**, Professor (School of Engineering), Kerala.
- III. **Dr. Ashwin Anil Gumaste**, Institute Chair Associate Professor (Computer Science and Engineering), Indian Institute of Technology, Bombay, Maharashtra,

Between December 16th, 2021, and February 2nd, 2022, the committee held deposition hearings for involved in the case as experts and petitioners are Mr. Sashi Menon, Hon. MP John Brittas, and Mr. Siddharth Varadarajan. When the Technical Committee's report was initially scheduled on May 20, it was extended until June 20, 2022. The Committee formally presented its conclusions to the Supreme court on August 2, 2022.¹⁴.

On August 25th, 2022, a bench chaired by Chief Justice of India (CJI) NV Ramana and Justices Surya Kant and Hima Kohli highlighted that while some malware was identified in 5 of the 29 devices, Pegasus was not one of those devices. This was after studying a lengthy report delivered by the three-member expert committee.¹⁵

The committee to investigate claims that the Indian government used Pegasus spyware has concluded that none of the 29 mobile phones it looked at contained any spyware.

The Committee's report made several recommendations, including passing legislation on

¹¹ Criminal Jurisdiction Writ Petition No. 314 OF 2021

¹² Ibid

¹³ Available at <https://timesofindia.indiatimes.com/india/pegasus-spyware-case-supreme-court-to-pronounce-order-judgment-today-all-you-need-to-know/articleshow/87297327.cms> visited on 8\05\2023

¹⁴ Available at <https://conventuslaw.com/report/india-the-pegasus-panaroma/>, visited on 08\05\2023

¹⁵ Available at <https://www.barandbench.com/news/no-pegasus-spyware-found-in-29-mobile-phones-examined-by-supreme-court-panel-some-other-malware-found-in-5-devices> visited on 08\05\2023

surveillance, protecting citizens' right to privacy, boosting national cyber security, and creating a procedure for voicing complaints about illegal surveillance.

committee continued by stating that the center government did not aid and cooperate with the inquiry committee.¹⁶

The committee report has been resealed and is currently being held in the care of the Secretary-General so that it can be checked for passages that might have implications for national security and to determine which passages of the report can be shared and which passages cannot. The Supreme Court could put a copy of the committee report online, but it has been done so under seal. The SC declared in its final statement that the case would be heard in 4 weeks.¹⁷

➤ **TRIPLE TEST** - The right to privacy was deemed to not be absolute, and any violation of that right must pass this test:

1. Justifiable goal
2. Correlation
3. Validity

- When these three ideas are applied to the Pegasus spyware outbreak, at least two of the three prerequisites are not met.
- The Pegasus spyware is not legal since it is not an existing and binding law and that it is not above the Supreme law of the land and this defies the last condition of the triple test or the condition of legality.
- There has not been any evidence of a rational link between the employment of Pegasus spyware and anything yet, but reports indicate that it was employed to kill a journalist and monitor the political opponents' tactics.
- The Pegasus spyware violates the final requirement of the triple test, which is the requirement of legality, because it is not a valid, binding law and is not superior to the Constitution.
- Since the Pegasus malware fails the three-part standard it is obvious that it is invading someone's privacy.

¹⁶ \Available at <https://conventuslaw.com/report/india-the-pegasus-panaroma/>, visited on 08\05\2023

¹⁷ Ibid

Impact of Pegasus Spyware Controversy: -

➤ **On fundamental rights:**

- The mere existence of a monitoring system impairs the enjoyment of the right to privacy as guaranteed by the Constitution.
- Articles 32 and 226 of the Constitution, which give the Supreme Court and High Courts, respectively, the authority to issue specific writs, are restricted when surveillance is only carried out by the government because it happens in secret.
- As a result, the harmed party is unable to demonstrate that their rights were violated.

➤ **Hinders the free flow of information:**

- It prohibits reading and exchanging unconventional, contentious, or provocative views.

➤ **Develops mistrust:**

- The personal security of journalists' sources is also put at risk by surveillance, especially for those who scrutinize the government. It fosters a climate of mistrust.

➤ **A BRIEF REVIEW OF PEGASUS-RELATED LAWS AND PRECEDENTS**

1. The Indian Telegraph Act's Section 5:

A public official now has the legal right to intercept communications in the interest of the general welfare. Such an interception cannot be unfounded because it must meet one or more of the following requirements.

- I. India's integrity and sovereignty
- II. Amiable interactions with foreign countries
- III. Public peace
- IV. Security of the State

The proviso to this provision states that intercepting press messages that are intended to be published and attributed to the Central Government or any State Government is prohibited unless specifically stated in this section.¹⁸

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

- All electronic data transmissions are subject to data interception under the IT Act.
- It permits the surveillance, decryption, and interception of digital data for the investigation of

¹⁸ S. 5, The Indian Telegraph Act, 1885.

an offence.

- It is noteworthy that the IT Act does not include the precedent-setting requirement from the Telegraph Act that "the occurrence of public emergency of the interest of public safety".

➤ **Protection of life and personal liberty [Article 21]:**

Article discusses the rights to life and individual freedom. the privacy right was added to the list of fundamental rights by the 2017 ruling in Justice K.S. Puttaswamy V. Uoi and is currently protected the Indian constitution¹⁹. The NSO Group claims that the only reason for its existence is to assist Governments in surveillance, but the current Union Government refuses to accept the list, claiming it to be false and without foundation. As a result, there is a clear violation of fundamental rights in the case of the Pegasus spyware. Personal information, such as conversations, images, videos, memos, and other data, have been extracted by the NSO Group.

➤ **CONCLUSION AND RECOMMENDATIONS:**

According to reports published by Amnesty International, the new Pegasus spyware outbreak has shocked everyone due to the Pegasus' possible targets. The alleged targets do not align with the NSO Group's objectives, who created the spyware known as Pegasus. The main goals of the Pegasus spyware are primarily to combat terrorism and improve the quality of life for everyone. The Pegasus spyware target list, however, does not align with the objectives as it consists of names of lawyers, activists, judges, and other professionals who work to improve the world rather than targets from terrorist organizations or those in positions of authority in unrest.

India urgently needs legislation that will prevent future Pegasus spyware and cyberattacks from giving users the ability to hack phones, access private data, and listen in on private conversations. Since citizens are the ones for whom such laws are enacted, if they are not at the benefiting end then such laws are of no use.

➤ **RECOMMENDATIONS**

➤ **Passing strict data privacy legislation:** A robust data protection law is required to safeguard each person's personal life and information from unauthorized government data gathering and surveillance.

➤ **Private spyware usage is forbidden:** A resolution to ban the use of Pegasus spyware would be a positive development.

¹⁹ Art 21, The Constitution of India.

➤ **judicial control over Pegasus** - A second branch of government should be established to provide oversight in order to attain the objective of fair legal procedure. judiciary can Determine if certain surveillance practices reference proportionate, assess the availability of alternatives, and strike a balance between the necessity of the government's goals and the rights of the people who may be affected.

➤ **References –**

1. Justice K.S. Puttaswamy V. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
2. <https://www.nsogroup.com/about-us/>,
3. <https://www.amnesty.org/en/latest/news/2021/07/the-Pegasus-project/>,
4. <https://conventuslaw.com/report/india-the-pegasus-panaroma/>,
5. <https://timesofindia.indiatimes.com/india/pegasus-spyware-case-supreme-court-to-pronounce-order-judgment-today-all-you-need-to-know/articleshow/87297327.cms>
6. <https://www.barandbench.com/news/no-pegasus-spyware-found-in-29-mobile-phones-examined-by-supreme-court-panel-some-other-malware-found-in-5-devices>
7. *navtej singh johar v. union of India* 2018) 10 SCC 1
8. *joseph shine v. union of India* 2018 SCC Online SC 1676