

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 3

2023

© 2023 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

The Impact of the Recent Pegasus Spyware Controversy on the Right to Privacy in India

SOUJAATYAA ROY¹

ABSTRACT

Pegasus is a Spyware developed by Israeli cyber-arms company NSO group that can be covertly installed on Mobile Phones (both Android and IOS devices). The spyware is capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target's device's microphone and camera, and harvesting information from apps. It is a Trojan Horse computer virus that can be sent "Flying through the air" to infect cell phones. The Pegasus espionage scandal first surfaced in July 2021. NV Ramana, the former Chief Justice of India, presided over the bench that heard the plea in Supreme Court. The SC established a committee after many hearings under the leadership of retired judge Justice RV Raveendran to look into the allegations.

Keywords: *Pegasus; Right to Privacy; Constitution; Spyware; Article 12; UDHR.*

I. INTRODUCTION

Spyware is a type of software that allows one user to secretly transfer data from another user's hard drive. Spyware is recognized as a malicious form of data collection.²

Pegasus is a Spyware developed by NSO group, which is a technology company based in Israel. The main purpose for which the spyware was developed and marketed was to help governments fight Crime and Terror. NSO group only sold the Spyware to governments. Pegasus software was first encountered in the phone of Arab Human Rights Defender, Ahmed Mansoor who received a text message which was followed by a link. He sent the link to Citizen Lab of the University of Toronto and after research it was found out that if Mansoor had followed the link then the spyware would have jailbroken his phone and implanted the spyware in a form of Social Engineering.

From 2016 since it was first encountered to 2021 when there was global outrage following the report, near about 50,000 telephone numbers were believed to have been identified by people of interest of clients of NSO and it became available to Paris-based media non-profit organisation namely, Forbidden Stories and Amnesty International. They shared the

¹ Author is a student at Adamas University, India.

² Termly, <https://termly.io/legaldictionary/spyware/>.

information with seventeen news media organisations and that was known as the Pegasus Project and a month long investigation was carried out and reported in Mid-July 2021. There was conclusive evidence to prove that many phones with numbers in the list was targeted with the Pegasus Spyware.

In 2021 French Intelligence (ANSSI) confirmed the remains of Pegasus spyware on phones of three journalists, including a journalist from France 24.³

A customer of NSO Group frequently hacked Lama Fakih's mobile phones on January 26, 2022, when she was looking into the 2020 Beirut explosion that claimed more than 200 lives. Lama Fakih is a US-Lebanese citizen and the director of crisis and conflict at Human Rights Watch.⁴

Pegasus Spyware was used to target and spy on heads of state, activists, journalists, and dissidents, allowing "human rights violations around the world on a massive scale". According to a joint investigation performed by seventeen media organisations in July 2021. Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates were also named as NSO customers in the study. The investigation also showed that journalists from several media outlets, including Al Jazeera, CNN, the Financial Times, the Associated Press, The New York Times, The Wall Street Journal, Bloomberg News, and Le Monde were selected for targeting with NSO spyware between 2016 and June 2021. It also identified at least 180 journalists from 20 different countries who were targeted in this manner.^{5 6}

(A) Research Questions

Whether the Pegasus Software invaded Right to Privacy in India?

(B) Hypothesis

The Pegasus Software invaded Right to Privacy as guaranteed by the Constitution of India.

(C) Literature Review

- **Constitutional Law of India- V.D. Mahajan⁷**

³ Kim Willsher, The Pegasus Project Surveillance, The Guardian (2nd August, 2021, 19:46 IST), <https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms>

⁴ Stephanie Kirchgassner, The Pegasus Project Beirut Explosion , The Guardian (26th January, 2021, 10:31 AM), <https://www.theguardian.com/news/2022/jan/26/human-rights-watch-investigator-allegedly-hacked-with-pegasus-spyware->

⁵ The Pegasus Project, Amnesty International (19th July, 2021), <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/>

⁶ Dana Priest, Craig Timberg and Souad Mekhennet, The Pegasus Project: A Global Investigation, The Washington Post (18th July, 2021, 8:15 PM), <https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/>

⁷ Sanjay Jain, V.D.Mahajan's Constitutional Law of India, 188-209, (Eight Edition,2023)

V.D. Mahajan's Book Constitutional Law of India is an authoritative text in the subject of Indian Constitution.

- **Pegasus Spyware Threat to Data and Cyber Protection Laws in India- Bhaswat Prakash⁸**

This article published in Legal Service India E-Journal opines relating to the history of the Spyware and details about the Pegasus Project.

- **Use of Spyware by Government Agencies: National Security or Cybercrime, A Huge Dilemma-Gaurav Sharma⁹**

This article published in Legal Service India E-Journal opines relating to cyber crime and right to privacy and reasonable restriction relating to right to privacy.

- **Right to Privacy and Data Protection under Indian Local Regime- Bandita Das & Jayanta Boruah¹⁰**

This research article published in SSRN talks about Right to Privacy under Article 21 as a Fundamental Right.

(D) Research Objectives

To analyse whether the Pegasus Software invaded the Right to Privacy In India.

(E) Research Methodology

The researcher in the present research has adopted Doctrinal or nonempirical method for collecting required data. The research will base its findings, inter alia, on analytical and critical studies.

II. RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

The Latin word "ius" was enlarged by the Decretum Gratiani in Bologna, Italy in the 12th century from "what is fair" to include "a right - an entitlement a person possesses to control or claim something," and this is where the idea of a human "right to privacy" first emerged.¹¹

⁸ Bhaswat Prakash, Pegasus Spyware Threat to Data and Cyber Protection Laws in India, Legal Services India E-Journal, <https://www.legalserviceindia.com/legal/article-6842-pegasus-spyware-threat-to-data-and-cyber-protection-laws-in-india.html>

⁹ Gaurav Sharma, Use of Spyware by Government Agencies: National Security or Cyber Crime, A Huge Dilemma, <https://legalserviceindia.com/legal/article-9222-use-of-spyware-by-government-agencies-national-security-or-cybercrime-a-huge-dilemma.html>

¹⁰ Bandita Das and Jayanta Boruah, Right to Privacy and Data Protection under Indian Local Regime, Volume 1, DME Journal of Law, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766 , SSRN - <https://ssrn.com/abstract=3827766>

¹¹ Right to Privacy, Wikipedia, https://en.wikipedia.org/wiki/Right_to_privacy#cite_note-SD-6

The right to privacy is a component of several legal systems that aims to regulate public and private activities that jeopardise people's privacy. ¹²The right to privacy is protected by more than 150 country constitutions. ¹³Although the right to privacy is not specifically mentioned in the Universal Declaration of Human Rights (UDHR), many people interpret this through Article 12, which reads: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation." ¹⁴ The UDHR was originally written to guarantee individual rights of everyone everywhere. The ICCPR¹⁵, the ICPRAMW¹⁶, and the UNCRC¹⁷ adopted the same language. Everyone is entitled to legal protection from these types of intrusions or assaults.

The Indian Judiciary also interpreted privacy rights as a fundamental right under Article 21 of Part III of the Constitution.

Following are the cases which dealt with Right to Privacy:-

*Kharak Singh vs State of U.P.*¹⁸

In this case, it was argued that the UP regulation's use of monitoring violates Part III of the Constitution's Fundamental Rights. After hearing this, the Supreme Court invalidated Regulation 236(b) because it allowed for monitoring via night time visits, which is an obvious infringement of an individual's ordered liberty and an unauthorised intrusion into their house. The other provisions of the law, however, remained valid since Article 21 does not apply because privacy has not yet been acknowledged as a basic right under the provisions of the Constitution. In contrast, J. Subha Rao argued that although while privacy was not recognised as a basic right, it was nevertheless a crucial component of Article 21.

*MP Sharma v. Satish Chandra*¹⁹

In this instance, the exercise of authority and seizure was contested due to a violation of the right to privacy. The higher judicial authority noted, however, that it was not the purpose of the Constitution's framers to restrict the power of search and seizure as a breach of fundamental private rights. The SC further clarified that the MP Sharma case did not answer any queries

¹² Samuel D. Warren and Louis D. Brandeis, Right to privacy, Harvard Law Review, Vol. 4, No. 5, 15 th December, 1890, <https://faculty.uml.edu//sgallagher/Brandeisprivacy.htm>

¹³ List of Constitutions, Constitute, https://www.constituteproject.org/constitutions?lang=en&status=in_force&status=is_draft

¹⁴ Universal Declaration of Human Rights, Article 12, 10th December 1948.

¹⁵ International Covenant on Civil and Political Rights, 1966.

¹⁶ International Convention on Protection of Rights of All Migration Workers, 1990

¹⁷ The United Nations Convention on the Rights of Child, 1989.

¹⁸ 1963 AIR 1295, 1964 SCR (1) 332.

¹⁹ 1954 AIR 300, 1954 SCR 1077.

about the Right to Privacy as a Fundamental Right under Part III of the Constitution. Therefore, under the Constitution, the right to privacy could not be recognised in this case.

*People's Union for Civil Liberty v Union of India*²⁰

In this case, the constitutionality of phone tapping on the grounds that it violates the right to privacy emerged. The Supreme Court ruled that telephone talks are covered by the right to privacy and that a call can be placed while seated anywhere, whether at home or at one's office, because these interactions are crucial to a man's daily existence. As a result, Article 21's Right to privacy is violated when phone calls are recorded. However, the State may record such conversations if there is a law directing the method to be used for telephone tapping or if it complies with the Telegraph Act's Rules.

Different types of privacy, such as the privacy of phone conversations and medical records, emerged as a result of this judicial interpretation. The majority of judges in the Kharak Singh and MP Sharma instances concluded that the right to privacy is not a fundamental right, hence it has not yet been recognised as such.²¹

Right to Privacy in India was recognised in the Writ Petition filed by K.S. Puttaswamy vs. Union of India²² or otherwise known as Aadhar Card Case. While this case was being heard, the controversy around right to privacy was yet again erupted, which resulted in the formation of a Special Constitution Bench which recognised Right to Privacy as basic Fundamental Rights of every Citizen.²³

III. PEGASUS SPYWARE AND HOW IS IT VIOLATING RIGHT TO PRIVACY OF CITIZENS

The Pegasus Project, widely regarded as the most advanced smartphone attack tool, has recently come under fire when it was revealed that over 50,000 people worldwide, including several in India, were the targets of cyber espionage. Additionally, the revelations mark the first time a malicious remote jailbreak exploit has been found inside an iPhone.

The main purpose of the Spyware is combatting terrorism and fighting crime but NSO claims that it can be used for other purposes as well.

According to a research by the online security provider Kaspersky, Pegasus is a modular piece of malware that has the ability to start full surveillance on the targeted computer. To put it simply, it installs the required modules to read the user's messages and mail, listen to calls,

²⁰ 1997 3 SCC 433.

²¹ Bandita Das and Jayanta Boruah, *Supra* note 9.

²² (2017) 10 SCC 1.

²³ Sanjay Jain, V.D. Mahajan's Constitutional Law of India, Eighth Edition, 2023, Pg. 194.

transmit back the browser history, and more, effectively gaining control of practically every part of your online life. All the info on your device is accessible since it can even listen in on encrypted voice and text files.

The latest Pegasus malware has "zero-link" technology, which means it doesn't require the user to click on any links in order to exploit zero-day vulnerabilities. Zeroday vulnerabilities are those that have just been identified in the operating system but which the developer is still not aware of. There are currently no fixes or updates that can protect a user because the vulnerability is still in its "day zero". NSO Group, the Israeli company that owns and developed Pegasus, takes advantage of these weaknesses to call or text the target's phone in order to deliver the spyware. Since the user doesn't need to do anything, the malware automatically installs itself on the phone. Pegasus bypasses even encrypted messaging applications like WhatsApp, and Telegram to grant access to the target's smartphone to NSO's "government clients" after it has been installed.

Since Pegasus gains access to the operating system, all phone activity can be observed when the device is turned on. It feels like someone is watching what you do on your phone from behind you. Without the user's knowledge, Pegasus operators may remotely capture audio and video from your phone, extract phone messages, utilise GPS to monitor your whereabouts, and retrieve passwords and authentication keys. A possible assault cannot be proven until a device is sent for forensic examination and specialists examine the data transmission to and from the phone. The tragic reality is that because Pegasus takes use of zero-day flaws, there is little that can be done to prevent security breaches until operating system developers proactively provide an update to your phone designed to shield you from sophisticated malware like Pegasus.²⁴

The phones of thousands of their loudest critics, including journalists, activists, politicians, and business executives in Mexico, Morocco, and the United Arab Emirates, were hacked using spyware created by NSO Group, according to a global consortium of news organisations.

A list of 50,000 phone numbers that was disclosed to Forbidden Stories also contains possible targets. The NSO's Pegasus malware, which has access to all of a person's phone's data, was found to have targeted dozens of victims, according to research done on their phones.

Activists, journalists, and officials in India had their WhatsApp accounts hacked, it was discovered in late 2019, and the Indian government was accused of being involved.²⁵

²⁴ Asif Muztaba Hassan, Pegasus Spyware: What it is and how does it work, *The Daily Star*, 19 th July 2021, 6:57 Pm, <https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/pegasus-spyware-what-it-and-how-does-it-work-2134001>.

²⁵ Anuj Srivas and Kabir Agarwal, *The Wire*, <https://thewire.in/media/pegasus-project-spyware-indian-journalists>.

Pegasus was used to target Indian journalists, activists, attorneys, and top government officials, Facebook, the parent company of WhatsApp, acknowledged on October 30, 2019. It was rumoured that the journalists and activists had been under surveillance. The journalists and activists were believed to have been targets of surveillance for a two-week period prior to the Lok Sabha elections.²⁶

The Indian IT Ministry asked WhatsApp for a thorough answer on the matter. WhatsApp reacted by saying that it has twice notified the Indian government of the security breach – first in May and once in September 2019. It was confirmed that 121 people in all had been the targets of the malware.²⁷

In Mid of 2021, a Writ Petition was filed in Supreme Court by Manohar Lal Sharma²⁸ which was accepted in the court and the SC appointed a Technical Committee to prepare and submit a report after thorough examination of the alleged persons phones. Out of 29 phones which were submitted before the court only 5 phones were found with some sort of malware but it was not clear whether it was Pegasus or not.²⁹ ³⁰SC did not reveal the report data publicly as the report contained personal data therefore the report was submitted with a closed seal.³¹

Pegasus Spyware is indeed a serious issue. It is the most powerful software of its type till date. Article 21 recognises every persons Right to Privacy and it has been deemed as a fundamental right in K.S. Puttaswamy case. Therefore, Pegasus Spyware if used by our government violated every alleged person's Constitutional Right.

Journalist Saurav Das requested information under the Right to Information (RTI) Act in October 2019 and questioned if the Indian government had bought or received a purchase order for the Pegasus malware.³²

"Please refer to your online RTI application dated 23.10.2019 received by the undersigned CPIO [Central Public Information Officer] on 24.10.2019," the Ministry of Home Affairs said.

²⁶ Chawla, Ajay, Pegasus Spyware – 'A Privacy Killer' (July 21, 2021). SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890657 .

²⁷ IBID.

²⁸ WRIT PETITION (CRL.) NO. 314 OF 2021.

²⁹ ET Tech, Daily Top 5, The Economic Times Tech, 25 th August, 2022, <https://economictimes.indiatimes.com/tech/newsletters/tech-top-5/sc-says-no-conclusive-proof-on-pegasus-it-firms-juggle-myrriad-issues/articleshow/93780996.cms?from=mdr>.

³⁰ Findings of the Pegasus Committee, The Indian Express, 26 th August, 2022, 7:40 IST, <https://indianexpress.com/article/explained/explained-sci-tech/supreme-court-verdict-pegasus-spyware-case-explained-8110710/>.

³¹ Dhananjay Mahapatra, Pegasus Project, Times of India, 26 th August, 08:08 IST, <https://timesofindia.indiatimes.com/india/supreme-court-picked-panel-finds-no-proof-of-pegasus-on-29-phones-it-got/articleshow/93786248.cms>.

³² The Wire Staff, 18 th July 2021, <https://thewire.in/government/project-pegasus-spyware-government-resonse-meity>.

It is advised that the undersigned CPIO does not have access to such information.³³

IV. CONCLUSION

Right to Privacy as guaranteed by the Indian Constitution is Fundamental Right of all citizens/persons. Pegasus Spyware can be used to invade privacy of every person and in many cases it has been seen so. Pegasus Spyware was first discovered in the phone of Emirati Human Rights Activist, Ahmed Mansoor. Since then the workings and functions of the spyware became more and more advanced to a level where it could be on someone's phone without being detected. The Pegasus spyware has access to all of the personal data on the phone of the target user. Even WhatsApp communications that are encrypted can be accessed by it. It may surprise you to learn that this malware is also capable of reading messages, tracking calls, monitor user behaviour within apps, collect user location information, and gain access to the phone's camera. In addition, the hacker can use the Pegasus malware to listen through microphones.³⁴ It can deliver any information as needed by its owner which in its very basic stage is violative of Right to Privacy.³⁵ Right to Privacy is a Fundamental Right and it is guaranteed in the case of *K.S. Puttaswamy vs. Union of India*, therefore if this spyware is used for spying on citizens it violates Right to privacy and goes against the very basic principles on which our Constitution was written upon.^{36 37}

³³ Prashant Pandey, An explainer on the Pegasus Software, News Click, 21 st July 2021, <https://www.newslick.in/An-Explainer-Pegasus-Spyware>.

³⁴ David Pegg and Sam Cutler, The Pegasus Project Surveillance, 18 th July 2021, 9:30 pm, <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>.

³⁵ M Drushika, Pegasus Spyware, Constitutional Law Society NLU Odisha, <https://clsnuo.com/2021/10/09/pegasus-spyware-an-invisible-threat-to-peoples-privacy-in-india/#:~:text=Pegasus%20is%20a%20proprietary%20surveillance,control%20over%20its%20user%20devices>.

³⁶ Pegasus Project, Human Rights Watch, 26 th August, 9:00 Am, <https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling>.

³⁷ Shubham Priyadarshi, Analysing the Pegasus Case, SCC Online, 7 th February 2022, <https://www.sconline.com/blog/post/2022/02/07/pegasus-case/>.