Page 1776 - 1784 **DOI:** *https://doij.org/10.10000/IJLMH.115986*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 5

2023

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

ANGEL SINGH[1]

ABSTRACT

The current world is run by technology and network connections. And in such a world where everything is becoming digital through everyday developments, it is crucial for us to know that everything we store on our personal devices are secure and there is no threat to our privacy. We must know what cyber security is and how we can use it efficiently and effectively. Our systems, devices, important files or documents, contacts, data and other important virtual things are at a big risk if there is no security to protect it. The development of latest technology and weaponized software presents considerable cyber security challenges, with the Pegasus spyware, developed by NSO which is an Israeli group, serving as a prominent example.

The Pegasus spyware is a malicious code which operates secretly, infiltrating the target systems without the knowledge of the user and extracts sensitive information. This research aims to investigate into the peculiar characteristics and consequences of the Pegasus spyware. It also explores its methods of generation, the extent of control granted, its potential for tracking and its ability to exploit zero-day vulnerabilities, without the user's engagement. This study also highlights the Pegasus spyware as a cyber security threat to the right to privacy in India due to its powerful surveillance capabilities and its limited traceability. This research provides acumen into the working of the Pegasus spyware system and paves the way for developing constructive measures and strategies to safeguard the systems and user privacy.

Keywords: *Pegasus spyware, zero-day vulnerability, zero-click attacks, right to privacy, Article 21, Indian constitution.*

I. INTRODUCTION

In an era marked by technological developments and advanced digital landscapes the question of cyber security and concerns over protection of individual rights, more importantly the right to privacy has taken a center stage. The Oxford English Dictionary defines privacy as "*a state in which one is not observed or disturbed by other people*". The recent Pegasus spyware controversy, has significantly impacted the right to privacy of individuals all over the world,

[1] Author is a student at Army Institute of Law, Mohali, India.

 [ISSN 2581-5369]

including India. There are allegations that governments including that of India have used the Pegasus software to surveil individuals such as journalists, activists, human right workers, politicians etc., which have sparked concerns about the infringement of right to privacy. In India the Right to privacy is protected by Article 21 of the Indian Constitution, which is an extension of Right to life and personal liberty[2].

The Pegasus spyware, developed by Israeli technology company, NSO group is a malicious software that invades a person's privacy and infects a person's device to collect sensitive data, and forwards it to a third party without the consent of the user. Such spyware is an invasion on an individual's privacy, dignity and freedom of the press and speech. The most recent report from Citizen Lab, a Canadian security organization at the University of Toronto, is that the Pegasus spyware infected the mobiles of at least 30 Thai activists to which the NSO group told the Washington Post, "politically motivated organizations continue to make unverifiable claims against NSO".

The Pegasus controversy is the latest example of how vulnerable we all are to digital prying. Nowadays, almost everyone carries their smartphones or mobiles with them as the main source of communication, storing sensitive and personal information, including contacts, important documents, photos, text messages and emails, which makes the smartphones prime target for hacking. Spyware can reveal our personal information to a third-party bypassing encryption that protects the data sent over the internet.

This research paper aims to find out what Pegasus is and how it really works, the impact of the spyware on the right to privacy in India, and what can be done to protect it.

(A) Research methodology

This paper is of descriptive nature and the research is based on secondary sources for the deep analysis into the controversy of the Pegasus spyware, it's origin and impact on the right to privacy in India. Secondary sources of information like articles, journals, online newspaper reports and websites are used.

(B) Review of literature

Pegasus is the most technical spyware in the history, which is made by the Israel based cybersecurity company NSO group. Security researchers have revealed evidence of attempted or successful installations of this spyware on the mobiles of activists, journalists, politicians, human right workers and business people, and as the months go by, more and more Pegasus

[2] Indian Const. Art. 21.

 [ISSN 2581-5369]

infections are emerging.

The end-to-end encryption is technology that scrambles messages or other information on your phone and unscrambles or discloses them only to the recipients' phone, which means any one who interrupts the messages in between cannot read them. Companies like Dropbox, Google, Meta, Microsoft, Twitter, Yahoo, are among the ones whose apps and services use end-to-end encryption. And to try to prevent such attacks, Apple has built a new lockdown mode into iOS 16, its iPhone software which arrived in 2022, and also in its upcoming MacOS Ventura.

A group of news outlets including the Washington post, Le Monde, and The Guardian, are calling it the Pegasus Project, led by Forbidden Stories which is an organization of journalists that works on stories after the original journalists or reporters were somehow silenced. In a detailed forensic run by the Amnesty International, 67 smartphones were found to be targeted by Pegasus spyware out of which 37 phones were tested positive for the infection.

The most powerful forces unleashed against the Pegasus is that of the US government. The Justice Department of the US has launched a criminal investigation into the Pegasus controversy, after a whistleblower said that NSO group had offered "bags of cash" for sensitive data and information from a US tech firm, Mobileum, the Guardian said. At least nine State Department officials who were either based in Uganda or involved in the matters associated with the African country were infected by the spyware.

The Pegasus controversy has put a lot of pressure on Israel. The US government took a strong recourse and blocked the sale of US technology to NSO by putting the company on the government's Entity List.

II. WHAT IS NSO GROUP?

NSO stands for Niv, Shalev and Omri, which are the names of the company's founders[3]. It is an Israeli cyber-intelligence firm. Hulio co-founded the company in 2010. NSO also offers other apparatus to locate where a phone is being used, defend against drones and mine law implementation data to detect patterns. This company licenses surveillance software to government agencies around the world. The company describes the role of its product on its website as helping "government intelligence and law-enforcement agencies use technology to meet the challenges of encryption" during terrorism and criminal investigations[4]. The company

[3] Cyber Intelligence for Global Security and stability, NSO Group, (Sept, 10, 2023, 11:50 AM), https://www.nsogroup.com

[4] Mitchell Clark, NSO's Pegasus spyware: here's what we know, The Verge, (Sept, 10, 2023, 12:05 PM), https://www.theverge.com/22589942/nso-group-pegasus-project-amnesty-investigation-journalists-activists-targeted

 [ISSN 2581-5369]

told the Washington Post that it only works with government agencies, to accomplish this, in 2011 it signed its first agreement with Mexico, used its product Pegasus to track down drug gangs. NSO group said that if it finds any evidence or instance of abuse of the Pegasus software it will cut off an agency's access. The New Yorker coverage argues that Pegasus is similar to military equipment.

NSO has been involved in other hacks, including a reported hack of Amazon founder Jeff Bezos in 2018. The company was also sued in 2018 for its alleged role in hacking the device of a journalist named Jamal Khashoggi, who was murdered that year, inside the Saudi embassy in Turkey.

The CEO of the NSO group told the Washington Post that "somebody has to do the dirty work" and that Pegasus is "used to handle literally the worst this planet has to offer".

III. WHAT IS PEGASUS?

Pegasus is the name for perhaps the most powerful piece of spyware or a hacking program ever developed, which is developed, sold and licensed to governments around the world by the NSO group. Once it has wormed its way into your phone or for that matter any device, it can turn into a 24-hour surveillance device. Pegasus reveals all to the NSO customers who control it, the text messages, data, photos, documents or files, videos, emails, contact list and can even record phone calls, it can secretly activate a phone's microphone or camera to record conversations and create new recordings, it can also easily access the GPS and track the location of the device, all without the knowledge or permission of the user. It has the capability to infect billions of phones running either on Android or on iOS operating systems. The spyware is designed to bypass the encryption and can mask its activity. Pegasus infects the device through so-called "zero-click" attacks that take advantage of vulnerabilities in software like Apple messages or Meta's WhatsApp to silently install software, which does not require any interaction from the phone's user to succeed. This means that a successful spyware attack on a device just needs an operating system along with a particular vulnerable app. NSO has invested substantial effort in making its software onerous to detect and Pegasus infections are very baffling. Pegasus is invented to penetrate devices running Android, iOS, Blackberry and Symbian operating systems and turn them into monitoring devices.

Pegasus was developed to combat terrorism and crime, but it is being misused as a cyber weapon in controversial espionage ambush on political figures, well known journalists and other civil society leaders.

 [ISSN 2581-5369]

IV. How does the Pegasus spyware work?

The first ever Pegasus attacks were recorded in 2014. And the fully working version of Pegasus, which was discovered in 2016, infected the smartphones using so-called spear phishing, text messages or emails that trick the target into clicking a malicious link that secretly installs the software. It can also be downloaded through a wireless transceiver located near the target. Another method used by the Pegasus to attack smartphones is the zero-day vulnerability. This is a vulnerability that the manufacturer is not yet apprised of, and does not require any action from the device user, such as fraudulently installing or granting permission. Yet another way used to attack devices consist of calling and sending text messages, when attempting to answer, the call was cancelled, however, even this call was enough for the malware to be installed on the smartphone or device and to get access to information stored on the device. Similarly, the virus could be sent through text messages and when the user opens the message, the spyware is installed in the device. Pegasus messenger uses the software, hacks it and creates a backdoor that leaves a loophole in the code of a legal program that provides a way into the device of the user for unauthorized activity and covertly lets the attacker into the system, giving administrator rights. Pegasus also has a capacity of self-destruction, which is activated in order to delete all the proof of existence of spyware on the device. The program entirely cleanses all traces of its manifestation, leaving nearly no chance of detection, this means that the device user does not require to grant any permission or in fact do anything at all[5]. For a successful spyware attack and installation all that is needed is a particular vulnerable app or operating system which is installed on the device, and it is known as the zero-click exploitation.

Once the Pegasus spyware in installed and infects the smartphone or a device of the user, it can theoretically harvest data from the device and disseminate it to a third party or back to the attacker. It can purloin photos, videos, location records, important files and documents, contact list, web searches, passwords, etc. It can automatically operate the cameras and microphones for real time surveillance, without the awareness of the user. Claudio Guarnieri, who runs Amnesty International's Berlin based Security lab, said, "Pegasus can do more than what the owner of the device can do".

V. Why is Pegasus in the news?

The Forbidden Stories, and Amnesty International, shared with 17 news organizations a list containing 50,000 phone numbers, who are believed to be of interest to NSO customers. The

[5] Marat Mussabekov, Pegasus spyware: what you need to know, Eurasian Research Institute, (Sept, 10, 2023, 03:32 PM), https://www.eurasian-research.org/publication/pegasus-spyware-what-you-need-to-know/

 [ISSN 2581-5369]

Pegasus Project, analyzed the phone numbers given in the list and recognized over 1,000 people in over 50 countries. From the data it was inferred that these phone numbers exhibited the signs of Pegasus spyware installation or attempted installation. The findings comprised of people who were outside of the NSO group's limitation to investigations of criminal and terror activity, and instead included business people, human right workers, journalists, executives, politicians, government workers etc.

According to the Washington Post, the list included the phone numbers of 10 prime ministers, three presidents and the king of Morocco, plus, 65 business executives, 85 human right activists, 189 journalists more than 600 politicians and government officials. The journalists include employees from Al Jazeera, CNN, Le Monde, The Financial Times, The Wall Street Journal.

The post also said that the Moroccan king was not the only royalty who became a target, a princess from Dubai along with her friends were also targeted and her attempt of gaining political asylum failed as she was allegedly kidnapped by the army commandos.

Pegasus infected the phones of at least 51 people in the Catalonia region in Spain, and six people working for Palestinian human rights group, the Citizen Lab revealed. Pegasus attacks on the phone of Jordi Sole, a pro-independence member of the European Parliament, and Elies Campo, a digital security researcher, according to the New Yorker.

The Guardian reported that the phones of two journalists at Hungarian investigative outlet Direkt36, were also infected.

The Pegasus spyware also attacked the mobile phones of Hanan Elatr and Hatice Cengiz, wife and fiancée of murdered Saudi columnist Jamal Khashoggi.

VI. Consequences of the Pegasus situation

The NSO group was black listed by the US Commerce Department, barring it from ingress to US technology, which is considered as a serious move as the NSO company needs computer processors, phones, and developer tools that come from US companies.

Apple sued NSO and telling them to locate and delete any private data its app collected, and calling it "amoral 21st century mercenaries"

Meta also sued the NSO group for allegedly targeting some 1,400 WhatsApp users.

According to Politico, the French President Emmanuel Macron changed his mobile phone number after his number appeared in the list of 50,000 number. He also raised the Pegasus spyware controversy with Naftali Bennett, the Prime Minister of Israel, the Guardian reported.

 [ISSN 2581-5369]

The journalists of Al Jazeera as well as other Mexican and Saudi journalists and activists, filed law suits against the company as spyware was used to hack their devices[6].

VII. WHAT DOES NSO HAVE TO SAY ABOUT THIS?

According to the Washington Post, the NSO admitted that their Pegasus software could be misused and that it had cut off two customers because of human rights abuses, in the recent 12 months.

The NSO co-founder, Hulio, told the Washington Post that, "every allegation about misuse of the system is concerning me". "It violates the trust that we give customers. We are investigating every allegation".

The company denied the claims about Pegasus and called them as false claims that were "based on misleading interpretation of leaked data". The company added that Pegasus "cannot be used to conduct cybersurveillance within the US.

The Washington Post reported, that, Dubai, Saudi Arabia, and Mexican government agencies were blocked by the NSO in the past from using the software[7].

NSO group called the media organization report as "full of wrong assumptions and uncorroborated theories".

VIII. HOW PEGASUS IMPACTED THE RIGHT TO PRIVACY IN INDIA?

There is a serious threat to the right to privacy of individuals due to the Pegasus spyware's capability to infiltrate the smartphones or devices without the user's permission, consent or knowledge and its ability to gather sensitive information from the device. This has infringed the Right to Privacy of the individuals, eroded the boundaries between personal and public spaces, and autonomy over their personal data. About 300 Indians become the target of the Pegasus spyware. It was discovered that Indian attorneys and activists had been targeted via WhatsApp. The phone lines of the opposition leaders such Rahul Gandhi and other top journalists were also being monitored by the Pegasus spyware. Over forty journalists, one constitutional authority, two sitting ministers in the administration of Prime minister Narendra Modi, three significant opposition leaders, current and past chief ministers, security organization officers, and hundreds of business people became the target of Pegasus, according to a report by The Wire.

[6] Pegasus: what you need to know about Israeli spyware, Al Jazeera, (Sept, 10, 2023, 03:35 PM), https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus

[7] Stephen Shankland, Pegasus Spyware and Citizen Surveillance: Here's What You Should Know, CNET, (Sept, 10, 2023, 03:07 PM), https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/

 [ISSN 2581-5369]

The Pegasus controversy has shed light on the exigency to strengthen the legal framework, and other techniques to ensure the responsible and ethical use of the surveillance technology. We need to find a right balance between cybersecurity and privacy rights, and use of such technology within the bounds of law. It has brig about considerations regarding the necessity of transparency and accountability mechanisms to avert misuse and make certain that technological developments do not come at the expense of fundamental rights of the individuals.

IX. THE RIGHT TO PRIVACY IN INDIA: A FUNDAMENTAL RIGHT

The fundamental right to privacy is one of the basic rights which is upheld in the Indian Constitution under Article 21, which guarantees the right to life and personal liberty and incorporates the right to privacy as an indispensable element.

In the case of **K. S. Puttaswamy vs. Union of India and Others** in August 2017, the Supreme court of India gave a landmark judgement and declared the right to privacy as a fundamental right. In this historic judgement, the Supreme Court held that privacy is a cornerstone and critical component of the judicial fights to come over the government's surveillance powers[8].

In **Kharak Singh vs. the State of U.P**., the supreme court in 1962, evaluated the impact of police monitoring in the form of domiciliary visits, which involved police entering the appellant's residence at night as infringing his privacy[9].

In **People's Union for Civil Liberties (PUCL) vs. Union of India**, the Apex court upheld that telephone tapping violated the basic right to privacy, thereby highlighting the right to privacy[10].

The Bombay High Court in the case of **Vinit Kumar vs. CBI**, held that monitoring a businessman's phone calls constituted an infringement of his right to privacy[11].

Therefore, in a democratic country like India, the Pegasus spyware is violating the fundamental rights of the citizens of the country. Such kind of a surveillance is an infringement on the right to privacy of an individual.

X. SUGGESTIONS

Strong legal framework: comprehensive laws should be enacted and enforced by the governments all over the world which explicitly address the concerns of digital surveillance, data breaches, and privacy violations.

[8] K. S> Puttaswamy (Retd.) and Anr. V. Union of India and Others, (2019) I SCC I.
[9] Kharak Singh v. State of U.P., 1963 AIR 1295.
[10] People's Union for Civil Liberties (PUCL) v. Union of India, AIR 1997 SC 568.
[11] Vinit Kumar vs. Central Bureau of Investigation, 2019 SCC Online Bom 3155.

 [ISSN 2581-5369]

Strengthen enforcement measures: the governments should establish impartial data protection authority which can look into grievances and impose certain fines for the violation of privacy.

Transparency and accountability: there should be regular audits and detailed reporting to ensure that the government uses surveillance in compliance with the law and should be held accountable for any violation of privacy.

User's education: government should make efforts to create awareness among citizens regarding the potential digital threats.

Fortify cybersecurity: to prevent hacking the governments should work to strengthen cybersecurity, by enhancing training and awareness initiatives.

XI. CONCLUSION

The Pegasus spyware controversy is a reminder of the delicacy of privacy in an era where the technology outpaces legal and ethical framework. The personal autonomy, liberty and privacy of an individual are all challenged and violated due to such invasive tools. There is an essential requirement of more rigid data protection laws or regulations and vigilant civil advocacy to mitigate the intrusion of surveillance and thus, ensuring to uphold the individual expression, fundamental rights, including the right to privacy and the democratic principles.

*****

 [ISSN 2581-5369]