Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Pegasus Judgement: Individual liberty vs National security

Shrihari Naik[a] Shreya Raj[b]

[a]Dr. BR Ambedkar National Law University, Sonipat, India [b]Dr. BR Ambedkar National Law University, Sonipat, India

Received 23 November 2021; *Accepted* 13 December 2021; *Published* 18 December 2021

Individual privacy Is a very important facet of any liberal democracy. The right is not absolute and the state can infringe upon it if necessary. The state hides in the blanket of national security and uses this exception to conduct authorised surveillance. On one end we have individual privacy and on the other, we have national security. The court in the ongoing issues over Pegasus controversy has been called upon to uphold and protect the fundamental rights of the citizens accorded to them under part III of the constitution. The government is also a party to the allegations. The lack of cooperation of the government has rendered the public clueless. The court in its judgment has discussed the ongoing issues of the citizens and also has tried to find a middle ground between individual privacy and national security. The same is comprehensively discussed below in the journal.

Keywords: *Pegasus, security, liberty.*

INTRODUCTION

Pegasus is malicious spyware installed on a computer or mobile without an individual's consent, damaging the system or stealing some sensitive data and transmitting that data to a third party. The Pegasus Spyware designed for the same was created by NSO Group, the Israeli cyber intelligence firm. The spyware infiltrates a smartphone be it Android, Blackberry,

iOS, or Symbian operating systems and gains access to everything which includes its camera and microphone too.[1]Claims have been made by the firm, that the spyware was made with the intent to help the government against terrorists and criminals, for targeted spying, not mass surveillance, the credibility of which is questionable at best.

HOW DOES IT WORK?

Pegasus looks for inconspicuous vulnerabilities or bugs in smartphones that even the latest security can't detect and prevent the phone from being infected. An earlier version of Pegasus (2016) was installed on the smartphone by spear-phishing i.e. tricking the user into clicking a link or opening a document that installs the software secretly via text messages or emails. Since 2019, the software can be installed with a missed WhatsApp call, which can even be deleted from the records afterward. Alternatively, a text message that produces no notification on the user's phone can also be sent, making it impossible for the user to detect it. This is known as the zero-click exploit. Another way to install the spyware is over a wireless transceiver located near a target. Once the installation is complete, Pegasus can extract any data from the device, transmitting it back to the attacker. The data could be anything ranging from photos and videos, location details, web searches, passwords, and call logs. It is also capable of turning cameras and microphones on for surveillance of the user without their consent or knowledge.[2]

THE PAST

2016: A Canadian cybersecurity organization, The Citizen Lab, found Pegasus on the smartphone of Human Rights activist Ahmed Mansoor.

2017: Carmen Aristegui, a Mexican journalist and the founder of Aristegui Noticias, an online news outlet, learned that she had been a target of Pegasus.

---

[1] Bhanukiran Gurijala, 'Wh at is Pegasus? A cybersecurity expert explains how the spyware invades phones and what it does when it gets in' (*The Conversation,* 09 August 2021) <https://theconversation.com/what-is-pegasus-a-cybersecurity-expert-explains-how-the-spyware-invades-phones-and-what-it-does-when-it-gets-in-165382> accessed 14 November 2021

[2] *Ibid*

2018: After Jamal Khashoggi, a Saudi journalist and critique had been killed, Omar Abdulaziz approached the court in Israel. He filed a lawsuit against NSO Group, claiming that they had sold the license of Pegasus to the Saudi government, which was used to spy on him. In September 2018 The Citizen Lab published a report identifying 45 countries where Pegasus was being used. India has made its entry in the list too as of recent.

2019: In October 2019, WhatsApp filed a case against the NSO Group, suing them. The claim was made that the software was being used by Pegasus operators for surveillance on users, which included journalists and human rights activists. WhatsApp requested the Department of Justice in the United States to launch an investigation.

2020: In December 2020, Citizen Lab published a report which contained the details of the use of Pegasus software by the government to spy on the phones of 36 Al Jazeera Journalists.[3]

THE PRESENT

On July 18th,2021, The Pegasus Project was published, an international journalism effort of 17 publications. The Guardian, Le Monde, The Washington Post, Süddeutsche Zeitung, Die Zeit, Aristegui Noticias, Radio France, Proceso, OCCRP, Knack, Le Soir, Haaretz/The Marker, The Wire, Daraj, Direkt36, PBS[4] contributed in the investigation conducted by a non-profit organization Forbidden Stories and Amnesty International's Security Lab. It was revealed that at least 180 journalists in 20 countries were targets of at least 10 clients of NSO Group. These government clients range from autocratic to democratic, in which India was also mentioned. It was revealed that in India, around 300 phone numbers were supposedly the target of the spyware including three opposition leaders, two ministers in the government, journalists, businessmen, human rights activists, scientists, and the legal community.[5]

[3] *Ibid*
[4] Phineas Rueckert, 'Pegasus: The new Global Weapon for Silencing Journalists' (*forbidden stories,* 18 July 2021) <https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/> accessed 18 November 2021
[5] *Ibid*

WHAT IS THE RESPONSE/ LEGAL STANDING?

NSO Group on Pegasus Spyware:

NSO has maintained that the surveillance software is sold solely to government entities. It also stated that the spyware sold to these governments was not operated by the firm, nor does it have access to any data collected of the targets. The identity of these government entities was kept under wraps. In response to the article published, NSO stated that it firmly denies the false claims made in the report, many of which raise serious doubts, questioning the reliability of the sources. The group wrote to forbidden stories and its media partners that the report published was based on "wrong assumptions" and "uncorroborated theories".[6] The firm commented that the sources have supplied the publishers with information that has no factual basis, as evident by the lack of supporting documentation for many of the claims made. According to the firm, the allegations were so outrageous and far from reality, a defamation lawsuit was being considered against the publishers. They also published a "Transparency and Responsibility Report" in June 2021[7]

Government Stand:

The center responded to the said allegations, saying the right to privacy of the citizens of India is an ensured fundamental right. The introduction of the Personal Data bill 2019 and the information technology rules 2021, for the protection of personal data of individuals, consolidates this fact. No unauthorized interception has been made by the government agencies, the allegations of surveillance on targeted people by the government have no truth or any concrete basis whatsoever but one of the preconceived conclusions. Further, stating that similar allegations were made in the past, of the government using Pegasus software on WhatsApp for surveillance.[8] The same was denied by all parties including WhatsApp in the Supreme Court, the reports holding no weightage. The news report at present is a similar case

[6] Editorial, 'Response from NSO and governments' (*The Guardian*, 20 July 2021) <https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments > accessed 14 November 2021
[7] *Ibid*
[8] *Ibid*

based on exaggerations and speculations made with a malignant intent towards the Indian Democracy and are completely misleading. India has a well-established procedure ensuring lawful interception, monitoring, or decryption of electronic communication. The requests for the same are made as per rules relevant under the provisions of section 5(2) of Indian Telegraph Act, 1885 and section 69 of the Information Technology (Amendment) Act, 2000.[9] Each case is approved by the competent authority, the Union Home Secretary at the centre and in the state governments, according to the IT (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.[10]

THE JUDGEMENT[11]

The court, in its order, starts with a famous quote by George Orwell. "If you want to keep a secret, you must also hide it from yourself." sets out to address the Orwellian concern of individual liberty and privacy against national security and state surveillance.[12] The court makes its intentions clear that's its efforts are to protect the fundamental rights of the citizens and not to commit judicial overreach[13] which may lead to judicial oligarchy.

ISSUES

Some petitioners have alleged to be the direct victim of the Pegasus attack, while others have raised issues regarding the inaction of the government to protect or give any clarity about the issue. Additionally, some petitioners have also raised apprehension that Pegasus software is only sold and used by the governments as per the comment made by the NSO Group, the creators of Pegasus. Most of the petitioners had sought an independent investigation.

LIMITED AFFIDAVIT BY THE GOVERNMENT

[9] 'Anatomy of the Pegasus spyware in India' (*ifex*, 23 July 2021) <https://ifex.org/anatomy-of-the-pegasus-spyware-in-india/> accessed 18 November 2021
[10] *Ibid*
[11] *Manohar Lal Sharma v Union of India & Ors* Writ Petition (Crl) No 314 of 2021
[12] *Ibid*
[13] Arfa Javaid, 'What is the difference between Judicial Activism and Judicial Overreach ?' (*Jagran Josh*, 11 May 2021) <https://www.jagranjosh.com/general-knowledge/difference-between-judicial-activism-and-judicial-overreach-1620741199-1> accessed 18 November 2021

The court on August 10 had asked the government to place an affidavit. The government responded with a limited affidavit stating time constraints. The government in its affidavit denied all the allegations made against it by saying the court can't evoke such an action while merely relying on some news reports and uncorroborated materials.

- The government said in its affidavit that the concerned issues were already cleared by the minister on the floor of the house.[14]
- The government submitted that the allegations were serious, and it will be willing to constitute an expert committee to investigate the matter.
- The government also indicated that the disclosure of certain facts will be determinantal to national security and that such information can be used against the state by terror groups to hamper national security.[15]

OBSERVATIONS BY THE COURT

The court on right to privacy:

The court in its observation emphasized the right to privacy, it reiterated that the right to privacy may be traced to the right to life under article 21 of the constitution.[16] The court stated that the right to life is not mere animal existence, but also provides a standard quality. Liberty is one of them. The court noted that the privacy of all the citizens is equally important as of these few journalists and activists. The court also stated that the fundamental freedom including the right to life and privacy is not absolute and the state can conduct surveillance while conferring to the guidelines laid out by the court in KS Puttaswamy's judgment.[17]

The said guidelines were:

- There must exist a law defining the procedure beforehand, the government cannot employ tools outside this specific bracket.

[14] *Ibid*
[15] *Ibid*
[16] *Ibid*
[17] *KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

- The aim of such invasion of privacy must be justified, and the action should not be disproportional.
- Proportionality, which ensures that the object and means of the action go in tandem with each other.
- The court acknowledged that the importance of surveillance and data in this digital age in the fight against terror. But it also cautioned that such surveillance can't be allowed blindly and should be done if necessary, and the due procedure under the existing laws must be followed.[18]

Right to Privacy v National Security:

The court quoted Daniel Solove to make a point regarding individual privacy vs state security. They mentioned that it should not be viewed as anything or all traded off, instead we should always strive for a middle ground and one must not be compromised for the other.[19]

Freedom of the press:

The court acknowledged the importance of the press in a democracy and said that freedom of the press is covered under freedom of speech. In its observation, the court further stated that the apprehension of the threat of surveillance over a journalist will undeniably hamper his performance and may result in self-censorship. Hence, a threat to freedom of the press is not only harming the rights of a few journalists, but also impacts society at large. It can undermine the press's ability to provide information to the public.

The court on lack of information:

The court noted the concern of the petitioners regarding lack of information. The court said that repeated reassurances have been made to the government that it will not be pushed to uncover information determinantal to the security of the state. Despite the state must this, the government has only responded through a limited affidavit, which does not shed any light on the government's stand and also fails to give any clarity to the facts at hand. The court said

[18] *Ibid*
[19] *Ibid*

such lack of action especially in a case concerning fundamental rights is alarming and cannot be accepted. Further, stating that the burden of the protection of the citizens' rights lies on the state and state must not hinder the court from rendering complete justice. The state cannot be an adversary, and the state must uncover all the facts and information to the court and the petitioners all the same.

The national security free pass:

The court, while acknowledging the government's stance on non-submission of the affidavit due to issues relating to security, states that it can't use this exception to national security as a free pass. National security cannot be the bugbear, mentioning which the Judiciary shies away. And the court to see if justice is done can take the path of judicial review. The government must plead and prove that the facts must be kept a secret as their divergence can affect national security mere invocation of national security will not render the court a mute spectator.

Order:

The court observed that as of now, there has been no specific denial by the government of any facts put forth by the petitioners. There has been only a vague denial in the limited affidavit, which cannot be sufficient. In such a case, the court has to accept the prima facie case made out by the petitioners and move ahead with it. The court passed an order to appoint an expert committee whose functioning will be overseen by a retired judge of the supreme court. The court also declined the plea to allow the government to constitute an expert committee since allegations are that union and state governments are parties to the deprivation of the right of the citizen.

CONCLUSION

The complete picture is yet to be painted, there are still some missing pieces to the story. It's not the first time that spyware/software has been used discreetly against human activists, journalists, and authoritarian figures. Though claims are made that this software helps the

government with surveillance to fight against terrorism and crime, more often than not the same is used to target journalists and human activists who are the voice of the public. Even if the government uses the veil of national security, is it necessary that it has to cost the public their rights? The NSO Group has officially declared that the spyware is sold only to Government agencies, not to private buyers. This raises several questions which have remained unanswered and unaddressed by the Government. No clarifying statement regarding the government's relationship with NSO Group or the use of Pegasus for surveillance on citizens has been made, despite the demands from the Supreme Court. The government has maintained its stand of not disclosing any information in the name of national security, even when the rights of the public, in general, are being infringed. The final judgment has yet to come, though whatever the outcome be, it cannot be denied that there is a need for reform in the surveillance aspects of national security. Without the adequate account of the Government, the citizens would always be vulnerable. The need of the hour is a Judicial oversight in our surveillance framework to avoid any chilling effect in the future where the rights of the citizens are unreasonably and illegally infringed.