

Vivekananda Institute of Professional Studies
Guru Gobind Singh Indraprastha University
Delhi, India

Pegasus: An infringement of right to
privacy

BURNISHED LAW JOURNAL

Rehan Bhasin

rehan.bhasin476@gmail.com

New Delhi, 110008

ABSTRACT

Pegasus spyware is created by an Israeli group NSO that aims to help Governments of different nations in surveillance, majorly to eliminate ill-doings in that country. However, opposite to the aims of Pegasus spyware, it is not used for the elimination of such activities, instead the use of Pegasus spyware has resulted in the infringement of the right to privacy of various individuals. For instance, it is under the allegation that the mobile phone of Congress party leader, Mr. Rahul Gandhi was attacked using the Pegasus spyware to look into the strategies adopted by opposition parties. As per the report published by Amnesty International, 50,000 renowned personalities worldwide are potential targets of this spyware, out of which close to 1,000 are Indians. The Pegasus spyware is a foundation to uproot the pillars of democracy, vanish the judiciary's independence, and suppress the people working towards reporting of ill-doings of people with power. The article looks into the reputable judgment of the Supreme Court in the case, Justice K.S. Puttaswamy V. Union of India facilitating the inclusion of the right to privacy in the Indian constitution. Furthermore, the Pegasus spyware has resulted in the infringement of various laws that are related to surveillance. However, it is pertinent to note here that the Union Government is reluctant to accept any such allegation and has termed the reports of such surveillance as “baseless, fake, and concocted”.

Keywords:-

1. Right to privacy
2. Pegasus Spyware
3. Surveillance

Pegasus: An infringement of the right to privacy

By: Rehan Bhasin

One of the most significant reforms in the history of Independent India is the inclusion of the right to privacy under article 21 of the Indian constitution. The right to privacy was a long lost cause for a prolonged period in the history of independent India. Right to privacy was mentioned in one of the rare instances by one of the renowned leaders of the Janta Party, Mr. Morarji Desai, the 4th prime minister of independent India. The imposition of emergency in 1975 by the Indira Gandhi government led to the arrest of various opposition leaders, journalists, activists, etc. One such leader was Mr. Morarji Desai. After the national emergency was revoked, journalists in large numbers gathered at the residence of Mr. Morarji Desai, looking at which he proclaimed, “This is a violation of my right to privacy”. This is one of the first instances where the term “right to privacy” was used.

However, India in the matter of the right to privacy, arrived a bit too late compared to other countries. Considering the current situation, the right to privacy has been protected as a fundamental right in the constitution of India by virtue of the 2017 judgment, Justice K.S. Puttaswamy V. Union of India.¹ The nine judge bench unanimously decided for protection of the right to privacy as a fundamental right under articles 14, 19, and 21 of the Indian constitution.

Recently, the right to privacy has been invaded by spyware called the “Pegasus (spyware)”. Pegasus has been created by an Israeli group, NSO. The Pegasus spyware is said to be one of the most dangerous attacks on cybersecurity which is by far a correct statement, since this spyware enters the mobile phone of the target person and extracts information like images, videos, conversations, notes, passwords, record videos, tracking GPS, etc. and gives access to such data to other persons. The spyware attacks both the popular operating systems, namely Android and IOS. The gravity of the spyware is such that the French president, Emanuel Macron, has changed his mobile phone after the announcement of this outbreak and after getting a note that he is one of the potential targets on the list of Pegasus spyware.² The NSO group claims that the spyware has been created to:-

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

² Pegasus spyware: French President Macron changes phone after hack reports, BBC, available at <https://www.bbc.com/news/world-europe-57937867>, last seen on 07/08/2021.

1. Prevent and fight terrorism
2. Preventing drug trafficking and breaking-up paedophilia
3. Find and rescue kidnapped children
4. Assist emergency search and rescue.³

But, the big question is the entry of this spyware into the electronic devices, how do they enter these devices? Earlier, this spyware used to join by clicking on certain links and URL's sent on WhatsApp, SMS, and iMessage in case of IOS devices. Still, now the spyware is much more upgraded and advanced that just a missed call on the mobile phone would open the doors for the spyware to enter and gain access to your device.⁴ A leaked list of 50,000 people has been revealed who are allegedly the targets of Pegasus spyware or are potential targets of Pegasus spyware out of which most of the names are of politicians, journalists, media houses, etc.⁵ Out of the 50,000 names from the leaked list disclosed by Amnesty International, 1,000 names are supposed to be Indian figures and out of those 1,000 names, 300 names have already been verified as the potential targets.⁶

The aims of Pegasus spyware as mentioned on the NSO website do not justify the names of the people as it consists of lawyers, academicians, opposite party leaders, journalists, etc. In 2018, a journalist, Jamal Khashoggi was assassinated on the order of Mohammed Bin Salman, King of Saudi Arabia as reported by the Central Intelligence Agency. Recently, it was alleged that the Saudi journalist Jamal Khashoggi was murdered by the Saudi Arabian Government and on an investigation, it was extracted that the pegasus spyware was installed on the mobile phone of the wife of the journalist months before the murder.⁷ Some known Indian names in the Pegasus spyware list are:-

³ Use cases, NSO GROUP, available at <https://www.nso.group/about-us/>, last seen on 07/08/2021.

⁴ ETtech Explainer: What is Pegasus spyware and how it works, available at <https://economictimes.indiatimes.com/tech/trendspotting/what-is-pegasus-spyware-and-how-it-works/articleshow/84607533.cms?from=mdr>, last seen on 07/08/2021.

⁵ 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 07/08/2021.

⁶ Two Union ministers, Rahul Gandhi, Prashant Kishor on Pegasus list: Report, available at <https://timesofindia.indiatimes.com/india/two-union-ministers-rahul-gandhi-prashant-kishor-on-pegasus-list-report/articleshow/84568453.cms>, last seen on 07/08/2021.

⁷ Revealed: murdered journalist's number selected by Mexican NSO client, available at <https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto>, last seen on 07/08/2021.

1. **Rahul Gandhi**- Member of the Lok Sabha
2. **Prashant Kishor**- Political strategist
3. **Ashok Lavasa**- Former election commissioner of India
4. **Umar Khalid**- Former leader of Democratic Students' Union in Jawaharlal Nehru University
5. **Rakesh Asthana**- Police Commissioner of Delhi
6. **Alok Verma**- Former Director of the Central Bureau of Investigation of India
7. **Anil Ambani**- Businessman

These are a few names out of the prolonged list of affected or potential targets. The most startling name among the list of targets is that of the woman and her eleven family members who had accused the former Chief Justice of India, Justice Ranjan Gogoi of sexual harassment due to which the pegasus spyware creates an apprehension on the spirit of democracy and the use of powers in a non-arbitrary manner. Even more shocking here is that the report claims that the Pegasus spyware has targeted 2 officers of the Supreme Court of India, lawyers, and even 1 sitting judge of the Supreme Court of India. However, the mobile number of the sitting judge is an old one but the judge was on the target list.⁸ If such claims are true then such practices make us question the independence of the judiciary and the spirit of democracy.

Moreover, there are reports of the year 2019 which claim that the Pegasus spyware was used to topple the Congress-JDS coalition Government from Karnataka which the NDA government led by B.S then took over. Yediyurappa.⁹ Further, there are allegations that nearly 300 phones were hacked using Israeli spyware during or before the general elections of 2019 which the BJP won by a thumping margin. The 300 phones that were alleged to be hacked were of people that were not “friendly” with the Modi Government.¹⁰

⁸ ‘2 SC officers, lawyers, old no. of SC judge on Pegasus list’, available at <https://timesofindia.indiatimes.com/india/2-sc-officers-lawyers-old-no-of-sc-judge-on-pegasus-list/articleshow/85056333.cms>, last seen on 07/08/2021.

⁹ Report links Pegasus to Cong-JDS govt collapse in 2019, available at <https://www.hindustantimes.com/india-news/report-links-pegasus-to-cong-jds-govt-fall-in-2019-101626807515626.html>, last seen on 07/08/2021.

¹⁰ How much of the data mined using Pegasus spyware help the BJP to win the 2019 elections?, available at <https://www.nationalheraldindia.com/opinion/how-much-of-the-data-mined-using-pegasus-spyware-help-the-bjp-to-win-the-2019-elections>, last seen on 07/08/2021.

HIGHLIGHTS OF THE JUDGMENT JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA

- The Aadhar judgment is one of the reforms that would go down in the history books of India as the Supreme Court once again emerged as the protector of Indian citizens. The judgment is historic in itself, but it becomes even more and even more crucial because it formed the basis of 2 more historical judgments that have further ensured equality to the citizens and greater freedom. The judgments are as follows:-
 - i. **Navtej Singh Johar V. Union of India-** This Supreme Court judgment decriminalized all consensual sex among adults, including homosexual sex in India.¹¹
 - ii. **Joseph Shine V. Union of India-** This Supreme Court judgment also scrapped an age-old section of the Indian Penal Code, 1860, and decriminalized adultery while scrapping off section 497 of the Indian Penal Constitution.¹²
- The judgment is more popularly known as the Aadhar judgment. Justice K.S. Puttaswamy a retired judge had filed a petition challenging the constitutional validity of Aadhar since it violates the right to privacy.
- The petitioner under this case argued that enforcing the use of Aadhar leads to an infringement of the right to privacy which is an intrinsic part of the right to life and personal liberty under article 21 of the Indian constitution. Further, the petitioner challenged the decision of the Supreme Court in the case **Kharak Singh V. State of UP and M.P. Sharma V. Satish Chandra**.
- In counter-arguments, the Government argued that the constitution nowhere guarantees individual privacy to the citizens. Moreover, the argument by the respondent was that the Aadhar act, 2016 only asks for certain personal information from the Indian citizens that ensures due surveillance by the State.
- The nine-judge constitutional bench upheld the petitioner's contentions and included the right to privacy under article 21 of the Indian constitution. It was held that the right to

¹¹ Navtej Singh Johar V. Union Of India, (2018) 10 SCC 1 (Supreme Court of India).

¹² Joseph Shine V. Union Of India, 2018 SCC OnLine SC 1676 (Supreme Court of India).

privacy is considered to be a, necessary fundamental right. Moreover, sections 57 and 33(2) of the Aadhar act, 2016 were deleted.

➤ However, the right to privacy was held not to be absolute and any invasion of the right to privacy must pass a triple test:-

1. **Legitimate aim**
2. **Proportionality**
3. **Legality**

If we apply these three principles to the pegasus spyware outbreak, we would find that at least 2 out of 3 conditions are not met.

Pegasus spyware's target list clarifies that the aim is certainly not legitimate, which defies the first condition of the triple test or the condition of a legitimate purpose.

No rational nexus is seen till now in the usage of Pegasus spyware as the reports suggest that the Pegasus is used for the assassination of a journalist, keeping an eye on the strategies of the opposition political parties, even keeping an eye on the sitting judge of the Supreme Court, etc and this defies the second condition of the triple test or the condition of proportionality as there seems to be no rational nexus between the object and means to achieve it.

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.

Thus, invasion by the Pegasus spyware is in clear violation of the right to privacy since it has failed in the triple test laid down by the Supreme Court of India.

➤ The Supreme Court overruled two of its own judgments namely:-

1. **M.P. Sharma V. Satish Chandra** in which it was held that the Indian constitution does not protect the right to privacy.
2. **Kharak Singh V. State of UP** in which it was held that the right to privacy is not protected under the Indian constitution to any degree.¹³

¹³ Justice K.S. Puttaswamy V. Union Of India, (2017) 10 SCC 1 (Supreme Court of India).

LAWS AND PRECEDENTS RELATED TO PEGASUS

The term “law” mentioned conforms with article 13(3) of the Indian constitution defining “law”. There are various sections of various acts that deal with the tapping of mobile phones. Tapping phones is not a recent affair or is not an affair that arose with the outbreak of Pegasus spyware. There are various precedents as well that are related to phone tapping. In 2013, the UPA Government committed that around 9,000 phone calls and 500 E-mails were intercepted daily. However, considering the current situation, the Union ministers claim that the lists released by Amnesty International are fake, baseless, concocted and that there is no proof whether the devices were hacked. Below the sections are mentioned are about the Pegasus spyware.

1. Section 5, the Indian telegraph act, 1885:

This section has provided authority to a public official to intercept communications in case of public emergencies or the interest of the public's safety and such powers. Such interception cannot be baseless as it must satisfy any one or more of the following conditions:-

- i. Sovereignty and integrity of India
- ii. Friendly relations with foreign states
- iii. Public order
- iv. Security of the State

Proviso to this section says that messages by the press that are intended to be published accredited to the Central Government or any State Government shall never be intercepted unless this section prohibits them¹⁴.

2. Rule 419A, Telegraph Rules, 2007:

As per this rule, the secretary to the Government of India at the Ministry of Home Affairs can pass orders of interception in case of matters relating to the center. A secretary-level officer who is in charge of the home department may intercept on issues relating to State.

¹⁴ S. 5, The Indian Telegraph Act, 1885.

Further, in unavoidable circumstances, an order may be passed by an officer who is not below the rank of joint secretary to the Government of India, duly authorized by the Union home secretary or the State home secretary.¹⁵

3. Section 69, Information Technology act, 2000:

This section allows for the interception, decryption, and monitoring of digital information in the interest of the following:-

- i. The sovereignty of India.
- ii. Friendly relations with a foreign state.
- iii. Defense-related matters.
- iv. Security of the State.
- v. Preventing the incitement of commission of any of the above.
- vi. Investigation of the offense.¹⁶

On the face of it, section 5 of the Indian telegraph act, 1885 and section 69 of the Information Technology act, 2000 look similar but the concept of section 69 of the Information Technology act, 2000 is wider than section 5 of the Indian telegraph act, 1885 since the requirement of the condition of satisfaction of public emergency or safety is not provided under this section, and the investigation by the Government officials under this section does not require any reasonable basis to resort to the method of surveillance.¹⁷

4. Rule 3, Information Technology (Procedure for safeguards for the interception, monitoring, and decryption of information) rules, 2019:

Rule 3 of these rules provides for the method or steps to be followed for interception under section 69(2) of the Information Technology act, 2000. Steps are summarised as follows:-

- i. Record the reasons for interception.

¹⁵ Rule 419A, The Telegraph Rules, 2007.

¹⁶ S. 69, The Information Technology Act, 2000.

¹⁷ Pegasus Spyware Scandal: Laws on Surveillance and Phone-Tapping, available at <https://www.livelaw.in/know-the-law/pegasus-spyware-scandal-and-laws-on-surveillance-phone-tapping-indian-government-and-it-act-178990>, last seen on 08/08/2021.

- ii. Direction for interception shall not exceed 60 days from the issue date, which may be extended up to 180 days.
- iii. Records are to be destructed obtained from interception within 6 months.
- iv. No disclosure is to be made to any third party.¹⁸

5. **Article 21 of the Indian constitution:**

The article talks about the right to life and personal liberty. By the 2017 judgment, Justice K.S. Puttaswamy V. Union of India, right to privacy was included in the list of fundamental rights and now has protection under articles 14, 19, and 21 of the Indian constitution.¹⁹ There is a clear violation of the right to privacy in the case of Pegasus spyware as the personal details, personal conversations, images, videos, memos, etc have been extracted by the NSO Group and the group claims that the sole purpose of their existence is to help Governments in surveillance but on the other hand, the current Union Government denies to accept the list claiming it to be fake and baseless.

6. **Personal data protection bill, 2019:**

The bill was introduced in December 2019 by the current Union Government. The personal data protection bill, 2019, came into the picture to respect the right to privacy of each individual residing within the territory of India. The bill seeks to protect the private data of each person living in the territory of India along with the unlocking of the data economy. On the face of it, the bill seems to be reform but with a deep study, one will come across a few flaws that have not been catered to. As per the bill's provisions; if there is any breach of data, then the victim whose data has been breached does not get any information regarding such breach. The service provider conveys the information to the regulator regarding the breach, the regulator decides whether to give information to the victim or not. Moreover, the personal data protection bill, 2019 has exempted government officials from its purview and has also empowered the Government to exempt any of its agencies.

¹⁸ Rule 3, Information Technology (Procedure for safeguards for interception, monitoring, and decryption of information) rules, 2019.

¹⁹ Art 21, The Constitution of India.

Despite the flaws, a data protection law must be in force in the country, but no urgency has been displayed till now by the Union Government to pass the bill even after the outbreak.²⁰

7. **People's Union for Civil Liberties V. Union of India:**

This case is infamously known as the phone tapping case. A petition was filed before the Supreme Court challenging the constitutional validity of section 5(2) of the Indian Telegraph Act, 1885. The writ petition was filed in consequence of the mainstream report regarding the tapping of political telephones published by the Central Bureau of Investigation. The petitioner contended that privacy is a fundamental right guaranteed under article 21 and article 19(1)(A) of the Indian constitution.

The court held that the authority to whom the order of interception is given may intercept for 60 days which may be extended to 180 days maximum. And the authority to which the order is given shall maintain the following records:-

- i. Communications that were intercepted.
- ii. The extent to which material is disclosed.
- iii. The number of persons and their identities to whom material is disclosed.
- iv. The extent to which material has been copied.
- v. The number of copies of the material.²¹

The court held that the right to privacy is an integral part of the right to life and liberty and that the act of tapping the telephone is inconsistent with the right to privacy.

Focussing on the judgment and the current Pegasus outbreak, there has been an infringement of the right to privacy of each person whose device has been hacked.

²⁰ Data protection bill, 2019 (Pending).

²¹ People's Union for Civil Liberties V. Union of India, AIR 1997 SC 568 (Supreme Court Of India).

CONCLUSION

The right to privacy forms part of the golden triangle of the Indian constitution. The golden triangle of the Indian constitution consists of article 14, 19, and 21, and the right to privacy has been included under article 21 which guaranteed the right to life and personal liberty to each person, moreover, the right to privacy has been guaranteed protection under article 14, 19 and 21 of the Indian constitution. This inclusion of the right to privacy as a fundamental right was by virtue of the 2017 judgment, Justice K.S. Puttaswamy V. Union of India. Moreover, as discussed earlier, the Pegasus spyware would also fail in the triple test of the right to privacy laid down by the Supreme Court of India. If any law satisfies the triple test, such law would gain the authority to abridge privacy.

The recent outbreak of pegasus spyware has left everyone in a state of shock because of the potential targets of the pegasus, as per the reports released by Amnesty International. The targets that have been reported are not consistent with the aims of the NSO Group, the developer of Pegasus spyware. The major objective of the Pegasus spyware is largely to fight terrorism and make the world a better place to live. But, the Pegasus spyware target list does not show consistency with the aims as it does not consist of targets from terrorist groups or people in power in disturbed areas rather it consists of names of lawyers, activists, judges, lawyers, etc that are responsible for making the world a better place. The mentioning of the serious incident of the assassination of Jamal Khashoggi is worth it here as that tells the malpractices done by the use of Pegasus spyware. Jamal Khashoggi was a Saudi journalist who was assassinated in the year 2018 on the orders of Mohammed Bin Salman. Later, it was found that Pegasus spyware was installed in the mobile phone of Khashoggi's wife months before the assassination. The twist is that Jamal Khashoggi was one such journalist in Saudi Arabia who used to report incidents of corruption occurring in Saudi Arabia. And even more shocking claims or even the most shocking claims of the Pegasus spyware report is that a sitting judge of the Supreme Court of India is under surveillance with the use of the Pegasus spyware resulting in closing the doors of independence of the judiciary.

If reports are to be believed then the spyware has been used in toppling the Karnataka government in the year 2019 and has also been used during the general elections of 2019. These two allegations have loosened the 4 concrete pillars of democracy. Transparency is far away from its actual place,

moreover, all these allegations have been denied by the Union government saying that such reports are fake and baseless which creates a greater apprehension that the spyware has been used for malpractices since the Pegasus spyware is a global outbreak.

India is in urgent need of a law that ensures that such cyber-attacks and any such future Pegasus spyware do not allow anyone to take benefit by hacking phones and getting into personal information and personal conversations. The Personal data protection bill, 2019 seems to be a step towards suppression of cyber attacks but the bill has certain flaws that should be rectified before the bill becomes a law, since, citizens are the ones for whom such laws are enacted and if they are not at the benefiting end then such laws are of no use.

