Jus Corpus Law Journal

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

Pegasus Snoopgate – 2021: Right to Privacy and State intrusion

Naman Tarun Khulbe[a]

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

Received 17 September 2021; *Accepted* 08 October 2021; *Published* 12 October 2021

Right to privacy is one of the fundamental rights that has been granted to all citizens of India. This right protects individuals from acts of the government and private organisations that threaten privacy. It is simply the right to be left alone. Government surveillance to the extent of spying on a citizen's personal life is a sign of authoritarian rule that can be disastrous for a democracy. If the government is left unchecked with the powers through which it can monitor and spy on its citizens under the pretext of preventing criminal activities, the result can be disastrous for the proper functioning of democracy and put citizens who value their privacy under grave danger. This is why there's a demand for better privacy protection laws in today's hi tech world where private data is easily accessible and can be misused if it gets into the wrong hands. This article will shed light upon one such instance of violation to right to privacy with alleged state involvement and also focus upon legality of government surveillance.

Keywords: *pegasus, privacy, state.*

INTRODUCTION

There are many methods of surveillance depending upon the mode and device targeted for monitoring. Some of the methods are computer surveillance, phone surveillance, social network analysis, data mining and profiling, wireless tracking, Internet of things. Surveillance by governments is mainly used for three purposes - intelligence gathering, prevention of

crime, and investigation of crimes. Instances of the government misusing its powers of surveillance and violating people's privacy even in the most democratic and liberal countries have come up from time to time be it the USA, UK, or India itself. The Pegasus snoop gate of 2021 was a global spyware scandal targeting several journalists, political dissenters, members of the opposition, activists, students and is one of the instances that shed light upon the value of data protection and privacy to safeguard free press and healthy democratic practices from authoritarian motives of the ruling government.

THE PEGASUS SNOOPGATE 2021

Pegasus is spyware developed by an Israeli security firm NSO group that can be used to covertly tap smartphones including devices running on Android and IOS. The spyware is a trojan horse virus that can be sent flying through the air" via messages, emails, etc hence the name "Pegasus" a Greek mythological horse with wings.[1] By 2016, it was confirmed that pegasus was able to read text messages, track calls, collect passwords, track location, access the microphone and camera of the target device, and collect information from apps[2].

The maker and distributor of the spyware, NSO group states that it furnishes the virus to authorized governments only for the usage of combating terrorism and serious criminal activities. It claims that under the terms of usage regarding its spyware in their contracts, it is specifically mentioned that their software shall be used for investigations related to national security matters and nothing else. Pegasus was first discovered in a failed attempt at hacking an iPhone of an investigative journalist in 2016. When it was discovered, it received considerable media coverage for its sophisticated surveillance techniques which had never been seen before. In July 2021, it was discovered that Pegasus was capable of hacking into an iPhone 12 running on a fully patched IOS version 14.6[3]. This shows that not even the most

[1] Max Boot, 'Opinion | An Israeli Tech Firm Is Selling Spy Software to Dictators, Betraying the Country's Ideals' (*The Washington Post*, 6 December 2018) <https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/> accessed 01 September 2021

[2] *Ibid*

[3] 'Forensic Methodology REPORT: How to CATCH NSO Group's Pegasus' (*Amnesty International*, 25 August 2021) <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> accessed 01 September 2021

secured devices on the market are safe from this spyware. In 2019, Whatsapp, the world's most popular messaging app and a subsidiary of Facebook revealed that over 1400 phones had been infected by malware sent via Pegasus by exploiting a zero-day vulnerability[4].

Claudio Guarnieri, head of amnesty international's Berlin based security lab had conducted an analysis of targeted phones leading to the revelation that NSO's constant search for weaknesses may have expanded to other commonly used popular apps such as Apple Music, gallery, messages. Once successfully hacked into a phone, Pegasus can extract data from any file be it address books, call history, internet browser history, calendar, messages. It virtually gains surveillance of overall activities conducted by phone.[5]

In 2018, Canada-based research organization citizen lab had revealed that NSO group categorized its operator customers and these customers had to be approved by the government of Israel before the sale of the software to ensure the software is not used against its own citizens. Few of these categorizations were revealed where countries of the Indian subcontinent were labeled under the term "GANGES". Similarly, countries from the middle east were labeled as "MIDDLE"[6]. According to the reports by citizen lab, operators in the Ganges category were associated with popular telecommunications providers from India, Pakistan and Bangladesh. Companies such as Bharti Airtel, Mahanagar Telephone Nigam Limited (MTNL), Hathway Cable Internet were named in the report to be associated with the spyware.

In 2020, a list containing over 500000 names classified as "Persons of Interest " by clients of the pegasus software was revealed to the public by Amnesty international and Forbidden stories, a media nonprofit organization based in Paris, France. The names of this list were passed along to 17 different media organizations under the umbrella name "project pegasus' '. The

[4] David Pegg & Sam Cutler, 'What Is Pegasus Spyware and How Does It HACK PHONES?' (*The Guardian*, 18 July 2021) <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones> accessed 01 September 2021

[5] *Ibid*

[6] A Kumar, 'All You Wanted to Know about Pegasus but Didn't Know Who to Ask' (*India Today*, 25 July 2021) <https://www.indiatoday.in/india/story/all-you-wanted-know-about-pegasus-spyware-controversy-nso-israel-india-1832051-2021-07-24> accessed 01 September 2021

Wire was the only Indian media organization to receive the list which contained names of 161 Indian targets. The full list was revealed to the public in July 2021 which resulted in shocking reactions across the political spectrum and the general public alike. These revelations are very concerning especially for a democratic country like India which has placed the right to privacy under fundamental rights. It is understandable for Arab monarchy states to have such a high level of surveillance over its citizens because of this power being allotted to those governments due to their nature of governance but when a democratic government such as the Indian government indulges in such authoritarian practices, the liberties and freedoms granted to citizens of such countries become threatened. Even the most important political figures such as Rahul Gandhi, the head of India's main opposition party, were not spared. Other prominent figures targeted by the spyware include Prashant Kishore, Ashok Lavasa, Stan Swamy, and many more.

The Supreme court of India took cognizance of the matter and decided to hear pleas from the petitioners alleging wrongdoing on the government's part. The supreme court observed that the allegations were "serious if newspaper reports are correct". At the same time, it requested petitioners to not engage in online debates and let the court hear the issue first[7]. It also directed the West Bengal government to suspend the enquiry committee set up to probe the hackings as the apex court is already hearing the matter. On 16 August, The central government filed an affidavit before the court saying that it will form an expert committee to probe the case.[8] The government however did not clarify who will constitute the committee or the timeframe for its investigation. The court expressed dissatisfaction with the affidavit as it failed to clarify whether the government used Pegasus spyware or not. Solicitor General Tushar Mehta responded to the court's observation by saying that aspects of national security are involved in this issue and that it will not be easy for the government to disclose sensitive information regarding the same on affidavits sought by petitioners. The Bench headed by Chief Justice of

[7] Dwivedi S and Srinivasan C, 'No Parallel Social MEDIA DEBATES': Supreme Court To Pegasus Petitioners' (*NDTV.com*, 10 August 2021) <https://www.ndtv.com/india-news/pegasus-case-supreme-court-tells-petitioners-dont-want-parallel-debate-in-social-media-speak-in-court-hearing-on-monday-2506867> accessed 05 September 2021

[8] *Ibid*

India N V Ramana said "it will discuss and decide the future course of action"[9]. The matter is still pending in court and will be heard in future.

RULING PARTY'S RESPONSE TO THE ALLEGATIONS

The Bharatiya Janata Party denied all allegations against the central government of spying on selected individuals. India's Minister of Electronics & IT , Ashwini Vaishnaw spoke in detail of the matter in the parliament claiming that there is no unauthorized surveillance by government agencies. He went on to say that government agencies have a complete set of interception agreements, including sanctions and surveillance by senior officials of the central and state governments for national interests, only for clearly stated reasons. The allegations that the government monitors certain people have no specific basis or facts. A statement issued by the central government stated that the media played the role of investigators, prosecutors and jury in this matter. The government shielded itself by showing how it passed the Personal Data Protection Bill, 2019,[10] and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[11] to shield the personal data of individuals and hence should not be on the receiving end for violating people's right to privacy.

Uttar Pradesh's chief minister, Yogi Adityanath reiterated the international conspiracy theory which he had earlier stated during questioning of his government over the Hathras rape case.[12] He claimed that "The opposition parties including the Congress are involved in dirty and controversial politics even when the country is amid a pandemic" He added, "The opposition, knowingly or unknowingly, is falling prey to the international conspiracy."[13]

---

[9] Express News Service, 'Pegasus: Centre Pleads National Security; SC Says Won't Force It' (*The Indian Express*, 18 August 2021) <https://indianexpress.com/article/india/pegasus-row-supreme-court-centre-7457708/> accessed 06 September 2021

[10] Personal Data Protection Bill 2019

[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

[12] Neha Lalchandani, 'International Conspiracy to Defame India: Yogi Adityanath ON Pegasus Row: India News - Times of India' (*The Times of India*, 20 July 2021) <https://timesofindia.indiatimes.com/india/international-conspiracy-to-defame-india-yogi-adityanath-on-pegasus-row/articleshow/84589477.cms> accessed 06 September 2021

[13] *Ibid*

LEGALITY OF GOVERNMENT SURVEILLANCE

The government of India has been allotted some surveillance powers under the Indian Telegraph Act, 1885,[14] which deals with interception of calls, and the Information Technology (IT) Act, 2000,[15] which deals with interception of data. Section 5 of the Telegraph Act,[16] allows central agencies to tap phones. The act says that such steps shall only be taken in times when sovereignty, security, and friendly relations with other countries with India are under threat.

In the ***public union for civil liberties v Union of India***,[17] the supreme court observed a lack of procedural safeguards. The court also noted the lack of maintenance of logs and records of phones tapped by the authorities under these provisions. The court held tapping as a serious tool in the invasion of an individual's right to privacy. Such powers can be granted for intelligence purposes however there have to be certain safeguards for the practice of such powers.[18] Based on these observations, there were amendments made to the act which introduced rule 419A. Rule 419A states that the authority to order interception of calls shall not be issued except by an order, in the case of the central government, the secretary of the union ministry of home affairs shall serve; if it is the state government, the secretary of the state ministry of home affairs shall serve. In unavoidable circumstances, such orders may be issued by officials not lower than the level of the Joint Secretary of the union government and duly authorized by the union home secretary or the state home secretary[19].

Hence if it is found out that the central government had authorised use of Pegasus spyware, it would be contradictory to it's claims now which deny any involvement in the snoopgate. The government then won't be able to take defence of practicing it's powers under the telegraph act since it is explicitly stated that such orders have to be authorised by the home ministry. Govt will also have to prove that there was a need to safeguard public safety since its existence is necessary to enact these provisions.

---

[14] Indian Telegraph Act 1885
[15] Information Technology Act 2000
[16] Indian Telegraph Act 1885, s 5
[17] *Public Union for Civil Liberties v Union of India* AIR 1997 SC 568
[18] *Ibid*
[19] Indian Telegraph Act 1885

Section 69 of the Information Technology Act,[20] and the Information Technology (Procedure for Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009,[21] allows interception, monitoring, and decryption of digital information for the investigation of an offense. For ordering the use of Pegasus, provisions from all of the above-stated acts need to be enacted to make that order lawful.

Violation of the right to privacy has also occurred if the allegations against the central government for using pegasus turned out to be true. In August 2017, The supreme court with a nine-judge bench ruled that the right to privacy is a fundamental right. The case name was ***Justice K. S. Puttaswamy (Retd.) and Anr. v Union Of India And Ors***[22]**.** The court stated the violation of this right by the state would be subject to the reasonableness test under article 14.[23]

The 'proportionality and legitimacy' test was also established under which 4 conditions have to be fulfilled if there's any violation of the right to privacy being conducted by the state -

- the state actions must be sanctioned by law.
- in a democratic society, there must be a legitimate goal of action.
- the action must be commensurate with the need for such intervention and
- subject to procedural safeguards that prevent abuse of the power of surveillance.

The question of how the mentioned targets of the spyware such as Rahul Gandhi, Mamta Banerjee, and other leaders of the opposition parties are a threat to the security of the nation will have to be answered as this condition is the biggest requirement to practicing violation of an individual's right to privacy by state-authorized orders. In the 2019 case ***Vinit Kumar v Central bureau of investigation***[24] , It was held that provisions provided under section 5 of the IT Act,[25] can only be enacted if there is an existence of "public emergency" or in the "interest of

[20] Information Technology Act 2000, s 69
[21] Information Technology (Procedure for Safeguards for Interception, Monitoring, and Decryption of Information) Rules 2009
[22] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* WP (C) 494/2012
[23] Constitution of India, art 14
[24] *Vinit Kumar v Central Bureau of Investigation* (2020) 1 AIR Bom R (Cri) 1

[25] Information Technology Act 2000, s 5

public safety". The court also held that if interception of Data is held outside the ambit of section 5 of the IT act, it will be mandatory for the said data to be destroyed. The procured data in violation section 5 will not be admissible in the court of law as well. The Data Protection bill, 2019 has also laid guidelines for data fiduciaries to follow while dealing with the data of Indian citizens. Section 12(1) of the bill,[26] states personal data can be processed by fiduciaries only if consent has been provided by the data principal. The consent should be free, clear, informed, specific, and capable of being withdrawn. The union government however can allow agencies to bypass provisions of this act in order to ensure security, public order, sovereignty and integrity of India and also in preserving friendly relations with other states. The provisions can also be bypassed to prevent commissioning of any cognizable offence[27].

CONCLUSION

Issues involving data protection and protection of the fundamental right of right to privacy have to be taken seriously. Especially when there is government involvement in such matters. There is no greater authority in a country than the government. People count on their elected representatives to safeguard their rights and liberties. Government should be the last entity to spy on a citizen. Recent cases of state intrusion into privacy have led to the belief that Indian democracy has fallen into peril. Observations made by the judiciary have been positive but not enough. The argument that interception of some suspected individual's data is necessary and helpful in the interest of national security to prevent crimes is understandable to some extent however there have to be certain safeguards and stringent regulations to ensure such power is not misused by the state. People targeted by the Pegasus software are opposition leaders and political dissenters. These are the major forces opposing the ruling government hence they are the most obvious targets to such Spywares if the government ever misuses its access over them to their advantage. The government should now prove that it was not involved in the scandal and also pass laws concerning data privacy.

[26] Data Protection Bill 2019, s 12(1)
[27] 'The Personal Data Protection BILL, 2019' (*PRS Legislative Research*, 6 September 2021) <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019> accessed 06 September 2021