UNLEASHING DIGITAL FORENSICS: EMPOWERING JUSTICE

Ananya Singh[*] Akanksha Priyadarshini[*]

INTRODUCTION

The case of Manohar Lal Sharma v. Union of India (UOI) and Ors.[1] centers around the alleged violation of the right to privacy due to the use of Pegasus software. The petitioners claim that individuals in India have been subjected to cyber-attacks and surveillance, with concerns raised about the involvement of either a foreign government or certain domestic agencies.

The primary issue before the court is whether an independent investigation should be conducted to examine the credibility of these allegations and ensure the protection of privacy rights. The right to privacy is a constitutional right in India, and limitations exist in its exercise, particularly concerning national security. The other issue which court has to answer is to create a balance of national security imperatives and individual privacy rights.

To investigate the Pegasus spyware allegations, the court formed a committee with technical expertise. The committee utilized digital forensics to analyze the allegations, highlighting the crucial role of technology in uncovering the extent of the surveillance. Digital forensics is essential in examining the presence and effects of Pegasus on targeted devices, revealing its operations, capabilities, and potential privacy violations. The findings from digital forensics investigations are crucial for establishing a case and validating the petitioners' claims, while also assessing the impact on the right to privacy. Overall, digital forensics plays a vital role in uncovering evidence, analyzing cyber-attacks, and providing valuable insights to the court in this case.

The case of Manohar Lal Sharma v. Union of India (UOI) and Ors. highlights the importance of protecting citizens' privacy rights while considering national security concerns and the importance of digital forensics by providing scientific and technical expertise to investigate the allegations surrounding the use of Pegasus spyware. The outcome of this case will have

[*]BSC LLB, FIRST YEAR, NATIONAL FORENSIC SCIENCES UNIVERSITY, GANDHINAGAR.
[*]BSC LLB, FIRST YEAR, NATIONAL FORENSIC SCIENCES UNIVERSITY, GANDHINAGAR.
[1] *Manohar Lal Sharma v. Union of India (UOI) and Ors* WP (Crl) No 314/2021

significant implications for the use of surveillance technology and the role of independent investigations in ensuring accountability.

BRIEF FACTS OF THE CASE

A group of petitions before the honorable apex court raises serious concerns about the privacy rights of individuals, which are at risk due to the possible use of Pegasus spyware on their devices. Pegasus Spyware is a powerful spyware developed by Israeli company NSO Group that can take over the entire functioning of a device and infiltrate it without the user's knowledge. Pegasus infections can be achieved through so-called “zero-click” attacks, which do not require any interaction from the phone’s owner in order to succeed[2]. In September 2018, Citizen Lab published a report that explained what Pegasus can do, and people from around 45 different countries were believed to have been impacted by this spyware suite.

On June 15, 2020, Citizen Lab and Amnesty International revealed a new spyware campaign that allegedly targeted nine people in India. Some of these individuals were already suspected targets in a previous spyware attack. Nearly 300 Indians were suspected targets and about 10 Indians’ devices are said to have undergone forensic examination in order to ascertain the presence of Pegasus Spyware to file the writ petitions.

On July 18, 2021, an investigation on the suspected use of the Pegasus Spyware on various private individuals was made public by a group of roughly 17 journalistic organizations. Respondents (Union of India) through the Hon'ble Minister of Railways, Communications and Electronics, and Information Technology denied all allegations made and emphasized the strict laws and regulations in India concerning surveillance and interception of communication. The Learned Solicitor General presented a "Limited Affidavit" that denied all allegations made against the Respondents (Union of India) and proposed to constitute a Committee of Experts to examine the issue raised. The honorable court found the "Limited Affidavit" insufficient and decided to establish a committee to conduct a comprehensive investigation and report its findings to the court.

[2] David Pegg and Sam Cutler, ‘What is Pegasus spyware and how does it hack phones?’ (*The Guardian*, July 18, 2021) <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones> accessed 28 May 2023

ISSUES INVOLVED IN THE CASE

The primary legal issue, in this case, concerns the protection of citizens' right to privacy as guaranteed under Articles 19[3] and 21[4] of the Constitution of India, 1950. The court must determine the scope of privacy protection and whether the alleged use of Pegasus software violates individuals' privacy rights.

Whether the petitions regarding the alleged spyware attack shall be accepted by this Hon'ble court?

Then the first issue raised by the petitioner was whether appropriate action is being taken by the Union of India after accusations surfaced concerning a potential cyber-attack on Indian nationals involved with the Pegasus spyware issue. The absence of any action taken against serious accusations made towards Respondent -Union of India has led many to question the government's commitment to protecting citizens' privacy and adhering to rule-of-law.

Whether an independent investigation should be conducted to maintain the credibility and impartiality of the process as the NSO group has disclosed it sold its Pegasus software only to vetted Governments, some foreign governments, or certain agencies of the Respondent-Union of India.

ARGUMENTS OF THE PARTIES

PETITIONERS

Mr. Kapil Sibal (Learned Senior Counsel)

Respondent (Union of India) shall not act in any manner which will make it difficult for the court to conclude and should not hold any information which puts the fundamental rights of the citizen at stake.

In 2019, reports of Pegasus hacking WhatsApp emerged, but no action was taken by the Respondents (Union of India). This lack of action raised serious concerns, as even an internationally respected organization acknowledged the evidence of such cyber-attacks without any prejudice against the nation.

[3] Constitution of India 1950, art 19
[4] Constitution of India 1950, art 21

Requested an independent investigation supervised by retired Judges to take place. The Respondents (Union of India) should only form a committee to inquire if the court-appointed committee investigating similar allegations would be free from the influence of the Respondents (Union of India)

Mr. Shyam Divan (Learned Senior Counsel)

Based on affidavits provided by two cybersecurity experts, he asserted that Pegasus had been utilized not just for surveillance but also for surreptitiously planting fabricated documents on targeted individuals' devices.

It is the Respondent's (Union of India) responsibility to further protect the interest of the individuals when such a national-level, large-scale cyber-attack had been made.

He also supported Mr. Sibal regarding the formation of a special committee for further investigating the probe.

Mr. Dinesh Dwivedi (Learned Senior Counsel)

The crux of Mr. Dwivedi's pleading was that if something is not specifically denied, it should be considered admitted. As the Respondents (Union of India) had never specifically denied the petitioners' allegations so same should be applied here and it should be deemed to be admitted by the Respondents (Union of India).

As Learned Senior Counsel was representing a reputed journalist he submitted before the honorable court that such an attack on the privacy of an individual is not just a breach of his fundamental right but also has a negative impact on the freedom of speech as a journalist.

Mr. Rakesh Dwivedi (Learned Senior Counsel)

If Respondents (Union of India) have not used any kind of spyware then it would have made the same statement on the limited affidavit provided but it did not do so. A committee should be formed to further investigate allegations made by the petitioners to get to the bottom of the truth.

Ms. Meenakshi Arora (Learned Senior Counsel)

Supported Mr. Sibal's prayer for forming a special committee to further investigate.

Mr. Collin Gonsalves (Learned Senior Counsel)

Highlighted the response of foreign governments to emphasize the seriousness with which they treated spyware attacks, underscoring the significance of the allegations.

Mr. M.L. Sharma (Petitioner in person)

This highlighted the fact that Pegasus Spyware is different from other spyware as it takes control over the entire functioning of the device and it can also be used to plant fabricated evidence.

RESPONDENTS (UNION OF INDIA)

The learned Solicitor General of India

The Minister of Railways, Communications and Electronics and Information Technology of India stated in Parliament on 18th July 2021 that the allegations of cyber-attack and spyware use had no factual basis. Based on the Minister's statements, it can be concluded that the allegations lack factual evidence and are considered baseless. Therefore, it is respectfully concluded that everything can be done at the behest of the Petitioner, especially considering that they have not presented a compelling case.

Placing such information on an affidavit which is asked by the petitioners will pose a potential threat to national security as the same could be used by the terror organization to hamper the nation's interest.

The committee should be allowed to be formed by the Respondents (Union of India) to investigate the allegations and its functioning will be completely independent and its credibility should not be questioned.

The learned Solicitor General submitted that only experts independent of any association with the Respondent-Union of India would be a part of the same, and there was no reason to question their credibility.

Finally, reiterated that this Court should allow the Respondent-Union of India to constitute an Expert Committee, which would be under its supervision.

JUDGEMENT

The Honorable Court held that in today's era of the information revolution, our entire lives are stored digitally. While technology can be beneficial, it also has the potential to intrude upon our privacy. Privacy is a legitimate expectation for individuals in a civilized democracy, not limited to journalists and social activists. Every citizen of India has the right to safeguard their fundamental right to privacy. The court must maintain the balance between the information collected by the state and on the other hand must protect the fundamental rights of its citizen. The contention of the petitioner is not about the use of personal data which can also be used by government agencies for use of national interest, but the bone of contention here is the misuse of spyware in violation of the privacy of the citizens.

The honorable apex court while adjourning the case held that

The Right to Privacy of an individual is not an absolute right it is always subjected to reasonable restrictions and the restrictions to be reasonable must pass through constitutional scrutiny. The fundamental right to privacy cannot be construed as absolute and must bow down to compelling public interest.[5]

The court on the other hand also recognized the individuals' Right to Privacy, by stating that any kind of espionage directly contradicts the individual's Right to Privacy.

The court further emphasized that the state cannot indiscriminately invoke national security as a means to escape accountability and unrestricted action. It must further plead and prove the facts to the court that the information which is being withheld contains issues relating to national security concerns.

The burden of the protection of the fundamental rights of its citizen always lies on the state.

The court accepted the petitioners' case of examining the allegations on the basis that no clear denial was made by the Respondents (Union of India), and the ambiguous denial in the name of a "Limited Affidavit" was insufficient.

Finally, the court asked for an Expert and Technical committee to be constituted to conduct a thorough inquiry and present it to the court.

[5] *Ritesh Sinha v State Of Uttar Pradesh & ANR* (2013) 2 SCC 357

The technical committee will comprise three members, including who are experts in cyber security, digital forensics, networks, and hardware, whose functioning will be overseen by Justice R.V. Raveendran (Former Judge Supreme Court of India) and he will be assisted by Mr. Alok Joshi (former IPS officer) and Dr. Sundeep Oberoi (Chairman, ISO/IEC JTC1 SC7).

The terms of reference for the committee to investigate were based on criteria such as whether spyware was used on citizens, whether any government agency or government was involved, details of the victim of the spyware, and whether any domestic entity or person was involved.

ANALYSIS AND CONCLUSION

ANALYSIS

"There will come a time when it isn't 'They're spying on me through my phone anymore. Eventually, it will be 'My phone is spying on me.

- Philip K. Dick"

Living in the constant fear of surveillance infringes upon an individual's fundamental right to privacy, eroding their sense of freedom and undermining trust in society. It is essential to protect this basic right to ensure a secure and democratic environment for all.

After several delays and forensic examination of the many devices, the committee submitted its report to the Supreme Court. The content of the report still remains confidential[6] and the final verdict is yet to come.

Many questions remain unanswered regarding the Pegasus spyware allegations. Despite the report submitted by the Supreme Court's technical committee, a final judgment is still pending, with the case losing its public attention over the years. The Pegasus case in India also brings attention to the government's failure to overhaul the surveillance law framework and enact robust data protection mechanisms since the landmark Puttaswamy v Union of India[7] ruling in 2017, which recognized the right to privacy as a fundamental right under the Indian Constitution 1950.

[6] 'Pegasus Committee Submits Final Report to Supreme Court' (*The Wire*, August 2, 2022) <https://thewire.in/law/pegasus-committee-supreme-court-report-submitted> accessed 28 May 2023

[7] *Justice K.S. Puttaswamy (Retd.) and Another v Union of India and Ors* WP (C) No. 494/2012

The Pegasus case highlights the critical role of digital forensics in uncovering evidence and arriving at a logical and scientific conclusion. The forensic tests conducted by Amnesty International found traces of Pegasus activity on 37 out of 67 phones examined, of which 10 belonged to Indian nationals providing crucial evidence that supports the allegations of illegal surveillance.[8] As technology continues to evolve, digital forensics will play a vital role in ensuring that individuals' rights are protected in the digital era.

In light of these concerns, an independent body should be established for the investigation as the United Nations special rapporteur on Counterterrorism and human rights recommended[9]. Such remedial bodies must have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

Legal provisions related to electronic surveillance attempt to balance national security concerns with individual privacy rights. The Telegraph Act allows the government to intercept messages only for specific purposes, such as public safety, sovereignty, friendly relations with foreign states, public order, etc. The interception cannot be used for political advantage or personal gain and must be temporary. Similarly, section 69 of the IT Act[10] empowers the government to issue directions related to the interception of any information via computer technology, but only for an investigation of an offense.

CONCLUSION

The evolving nature of privacy rights requires continuous adaptation of legal frameworks to keep pace with technological advancements. As surveillance capabilities expand, courts and policymakers must address the challenges posed by emerging technologies, strike a balance between security and privacy, and safeguard individual rights in the digital era. However, the Pegasus case in India has exposed the limitations of these legal frameworks and the need for stronger oversight mechanisms to prevent abuses of power and protect privacy rights in the

[8] 'Forensic Methodology Report: How to catch NSO Group's Pegasus' (*Amnesty international*, July 18, 2021) <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> accessed 4 June 2023

[9] 'India: Spyware Use Violates Supreme Court Privacy Ruling' (*Human Rights Watch*, August 26, 2021)<https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling> accessed 28 May 2023

[10] Information Technology Act 2000, s 69

digital era. This case also serves as a reminder of the importance of employing scientific methods and expert analysis to uncover the truth and hold those accountable for their actions.