MANOHAR LAL SHARMA VS. UNION OF INDIA AND ORS.

Case Citation: AIR 2021 SC 5396

Decision Date: 27 October 2021

Bench Strength: 3

Number of Opinion(s): 1

Aspect(s) of Privacy: Surveillance, Informational Privacy

Legal Provision(s): Articles 19(1)(a), 21 and 32(1) of the Constitution of India, 1950 ("Constitution")

Case Status: Not Overruled

Case Type: Criminal Writ Petition

"It is a settled position of law that in matters pertaining to national security, the scope of judicial review is limited. However, this does not mean that the State gets a free pass every time the spectre of "national security" is raised. National security cannot be the bugbear that the judiciary shies away from, by virtue of its mere mentioning. Although this Court should be circumspect in encroaching upon the domain of national security, no omnibus prohibition can be called for against judicial review."

Case Brief

In this case, the Supreme Court of India ('Court') examined allegations relating to the potential violation of the right to privacy of Indian citizens through the use of spyware technology. The case is related to the Pegasus suite of spyware ('Pegasus') developed by an Israeli technology firm ('the NSO group'). Pegasus could allegedly infiltrate digital devices and obtain real-time access to stored data, operate its camera and sound recording functions, and remotely control the devices.

The present batch of Writ Petitions arose in light of the alleged use of the spyware on private individuals in India. 300 mobile numbers belonging to Indians were allegedly under surveillance using Pegasus, including those of senior journalists, doctors, political persons, and Court staff. The NSO group reportedly only sold Pegasus to vetted governments. The Petitioner in this case argued that the use of Pegasus violated the Petitioners' rights to privacy and free speech. They sought an independent investigation into the allegations that Pegasus was deployed by foreign governments, or agencies of the Indian government against the citizens of India.

The Court formulated a three-member Technical Committee to undertake an independent enquiry into the petitioners' allegations. The Committee was also tasked with looking into the legality of any such deployment and providing recommendations on the existing surveillance and privacy framework in India. The Committee submitted its report to the Court in July 2022, after which the Court listed the matter for further hearing.The Court also examined the extent to which the Union of India could refuse to disclose information on the grounds of national security. It held that even if the State had a legitimate reason for not disclosing relevant information, it had an obligation to plead its case and prove that the information could not be publicly divulged.

Case Summary

Facts

In 2018, Citizen Lab, a laboratory based out of the University of Toronto revealed that the phones of individuals from nearly 45 countries were suspected to be infected by the Pegasus suite of spyware. Pegasus could allegedly obtain real-time access to all the data stored on the digital device, and could also remotely control devices. In 2021, a consortium of journalistic organisations from around the world published results indicating the use of the Pegasus spyware on private individuals. The published results indicated that out of around 50,000 leaked phone numbers that were allegedly under surveillance by clients of the NSO Group, nearly 300 reportedly belonged to Indians. The NSO Group reportedly only provided Pegasus to certain vetted government intelligence and law enforcement agencies.

The present batch of Writ Petitions were filed before the Court seeking independent investigation into allegations that Pegasus was deployed by foreign governments or the Union of India on the citizens of India. Petitioners argued that the use of Pegasus violated their rights to privacy and free speech.

The Union of India filed a 'limited affidavit' to the Court which denied all the Petitioners' allegations, and stated that it would constitute a Committee of Experts to examine the issues raised by the Petitioners. It refused to provide more information on the alleged use of Pegasus citing national security concerns.

Issues

A) Whether the State could refuse to provide information on grounds of national security in proceedings involving fundamental rights.
B) Whether the Union of India or its agencies used the Pegasus suite of spyware to surveil Indian citizens.

Decision

The Court noted that surveillance or spying by an external agency or by the State directly infringes the right to privacy of the citizens. It observed that the right to privacy was not absolute, and that the State may need to access information by interfering with an individual's right to privacy, provided that the measures used passed constitutional scrutiny. It referred to the three-fold test of legality, necessity, and proportionality laid down in *K.S Puttaswamy vs. Union of India ((2017) 10 SCC 1)* in this context.

Moreover, the Court noted the importance of the free flow of information between Petitioners and the State in writ proceedings before the Court. It observed that the State could refuse to divulge some information in the interest of national security and other grounds under Article 19(2) of the Constitution, However, it held that the State would have to include these constitutional concerns and grounds in its pleadings before the Court. It also noted that the State would have to prove that providing information would affect national security concerns.

In the present case, the Court accepted the *prima facie* case made by the Petitioners, since the Union of India did not specifically deny the facts presented by them. It noted that the 'omnibus and vague' denial through the 'limited affidavit' filed by the Union of India was insufficient in this regard. Consequently, the Court constituted a three-member Technical Committee overseen by a retired judge of the Court. The Committee was tasked with investigating the Petitioners' allegations relating to the use of the Pegasus suite of spyware on Indian citizens. It was also required to make recommendations on securing the right to privacy, and improving laws and procedures on surveillance in the country.

The Technical Committee submitted its report to the Court in July 2022. The matter was thereafter listed for further hearing.