Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Case Comment: When Privacy Meets Surveillance: Analysing the Manohar Lal Sharma Case

Chandrika Rao Gadicheria[a]

[a]University of Mumbai Thane Sub-Campus, Thane, India

Received 20 August 2025; *Accepted* 20 September 2025; *Published* 24 September 2025

INTRODUCTION

Ever since the rise of the internet and digital era in the early 2000s, there has been an increasing rise in privacy concerns as well. Privacy, as any layman would describe it, would mean any individual's right or privilege to retain their personal matters and affairs a secret.[1] Today, privacy is considered a basic human right and, in India, even a fundamental right; however, paradoxically, privacy is also treated as a privilege to a certain extent, not attainable by all. In the landmark case, K.S. Puttaswamy v Union of India (2017), it was recognised as a fundamental right. Yet, in practice, privacy remains; it rarely gets the respect it deserves, as governments and institutions often brush it aside in the name of security, convenience, or control. The controversy surrounding the recent Pegasus spyware scandal presented the Supreme Court of India with one of the most significant challenges to the right to privacy in recent times. The Manohar Lal Sharma v Union of India[2] case involves issues at the intersection of privacy, state power, and constitutional freedoms. This case commentary

[1] 'privacy' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/privacy> accessed 02 August 2025

[2] *Manohar Lal Sharma v Union of India* (2021) SCC OnLine SC 985

delves into this case and aims to critically analyse the Hon'ble Supreme Court's judgment. Furthermore, it sheds light on the evolving discourse on privacy in India and the challenges posed by surveillance in the digital age.

BACKGROUND OF THE CASE

Pegasus is basically a spyware that was developed by an Israeli Cyber-intelligence firm, NSO. A group that claims to develop technology for the government to protect people from terrorism and other crimes. This all began back in the year 2018. In September, the Citizen Lab at the University of Toronto published its Hide and Seek report[3], which first mapped Pegasus spyware's operations across 45 countries, exposing how governments were deploying it against journalists, activists, and political opponents under the guise of national security. At that stage, Pegasus was largely understood to work through malicious links that required the victim to click. In October 2019, Facebook[4] (now Meta) initiated proceedings against NSO Group in a U.S. federal court, alleging that the company had exploited WhatsApp vulnerabilities to deploy Pegasus spyware. While the suit did not specifically establish usage in India, it showed NSO's capabilities and modus operandi, eventually leading to subsequent concerns once the Pegasus Project revelations emerged in 2021.

The issue resurfaced in July 2021, when the Pegasus Project, a collaborative investigation by 17 international media organisations along with Amnesty International, revealed a leaked database containing over 50,000 potential targets. Later in September, Citizen Lab, working with Amnesty International, uncovered that Pegasus had evolved to employ far more insidious zero-click exploits, most notably the forced entry vulnerability in Apple's iMessage, which allowed silent infiltration without any user interaction. This escalation turned Pegasus from a sophisticated surveillance technology into a dangerous threat to digital privacy, triggering public outrage worldwide and ultimately leading to the litigation before the Supreme Court of India. In India, there were findings that Pegasus traces had been discovered on the phones of its own editors, political strategist Prashant Kishor, and several others. Citizen Lab confirmed traces on some devices of journalists, but for Prashant Kishor, it's a potential target or alleged traces, not a fully verified infection.

[3] Bill Marczak et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries* (Report No 113, 2018)
[4] *WhatsApp Inc v NSO Group Technologies Ltd* [2021] 17 F.4th 930 (9th Cir)

The database also allegedly included prominent figures such as Rahul Gandhi, Abhishek Banerjee, journalists like Siddharth Varadarajan, Paranjoy Guha Thakurta, activists, bureaucrats, and even a Supreme Court staffer linked to the 2019 sexual harassment allegations against then CJI Ranjan Gogoi. Opposition leaders and the Supreme Court staffer were potential targets, but not confirmed to be definitively hacked. On July 22, 2021, IT Minister Ashwini Vaishnav dismissed the reports as unfounded, emphasising that surveillance in India was subject to the Telegraph Act, 1885[5] and the Information Technology Act, 2000[6], both of which he claimed provided sufficient safeguards despite it being alleged that he was a potential target himself, according to the leaked database.

Meanwhile, around the same time, multiple petitions were filed before the Supreme Court. Manohar Lal Sharma, a lawyer from Delhi, was the first petitioner to approach the Supreme Court in July 2021 after the media reports surfaced, demanding an investigation into the alleged surveillance. Other petitioners included journalists such as N. Ram and Paranjoy Guha Thakurta, civil society representatives like Jagdeep Chhokar, and parliamentarian John Brittas. They sought an independent judicial investigation into whether the government had authorised the use of Pegasus, arguing that such surveillance would violate free expression and the constitutional right to privacy.

ISSUES RAISED

1. Whether the Supreme Court should direct an investigation to ascertain if the Union Government deployed Pegasus spyware.
2. If the Union Government did employ Pegasus spyware, whether such use constitutes a violation of the constitutional right to privacy.
3. If the Union Government did employ Pegasus spyware, whether such use contravenes any applicable legal or statutory framework governing surveillance.

DECISION

The Supreme Court constituted a three-member technical committee, led by former Justice R.V. Raveendran, to investigate the allegations of unauthorised surveillance using Pegasus spyware. The committee's mandate was to determine whether the spyware was used to

[5] Indian Telegraph Act 1885
[6] Information Technology Act 2000

infiltrate Indian citizens' devices, identify the entities responsible, and assess the legality of such actions. The Court directed the Union of India to file a detailed affidavit addressing these allegations. However, Solicitor General Tushar Mehta only submitted a limited affidavit, outright denying the accusations and arguing that the petitions relied solely on speculative media reports. The affidavit further proposed the creation of a government-appointed committee to examine the matter, ostensibly to prevent the spread of misinformation. The Supreme Court found this response inadequate, observing that it failed to clarify the Union's official stance. The Solicitor General contended that any further disclosure would compromise national security, but the Court remained dissatisfied. So it decided to constitute its own Technical Committee under the supervision of Justice R.V. Raveendran, a former judge of the Supreme Court, assisted by experts in cyber security, forensics, and information technology from leading institutions. This committee held depositions of petitioners and experts, including MPs and senior journalists, between December 2021 and February 2022. Initially required to submit its report by May 20, 2022, the Committee was granted extensions until June and eventually presented its findings to the Court in late July 2022.

LEGAL LACUNAE

First of all, India does not have a standalone law regulating state surveillance for citizens. The current powers derive from archaic statutes. For instance, the Telegraph Act, 1885[7], grants the government the ability to intercept communications for public emergency or sovereignty/security reasons. This act allows the government to intercept messages during public emergencies or in the interest of public safety.

While the Information Technology Act 2000 allows monitoring of electronic communications, it has vague procedural safeguards. Section 69[8] of the Information Technology Act, 2000 (IT Act), empowers the government to intercept, monitor, or decrypt information in the interest of national security, sovereignty, and public order. However, there is no requirement for prior judicial authorisation before surveillance activities are conducted. No independent body monitors or reviews surveillance activities, leading to potential misuse without accountability. And there is no dedicated law addressing the use of spyware like Pegasus,

[7] Indian Telegraph Act 1885
[8] Information Technology Act, 2000, s 69

leaving a regulatory vacuum. These deficiencies were brought to light during the Pegasus revelations, where it was alleged that the Indian government used the spyware to target journalists, activists, and political opponents.

ANALYSIS

The problem is that there is no clear framework for oversight, authorisation, or accountability, unlike in the United States of America or the EU (European Union). The U.S. has a structured framework for surveillance, primarily under the Foreign Intelligence Surveillance Act of 1978[9]. This act established the Foreign Intelligence Surveillance Court (FISC), comprising federal judges appointed by the Chief Justice of the U.S. Supreme Court. Agencies must obtain a warrant from FISC before conducting surveillance on foreign targets. This act also outlines procedures for electronic surveillance, physical searches, and the collection of foreign intelligence information. The act has been amended, notably by the USA PATRIOT Act[10] and the Foreign Intelligence Surveillance Amendments Act of 2008, to address evolving security concerns. While this act provides a legal framework, it has faced criticism over issues like bulk data collection and the scope of surveillance on U.S. persons.

Meanwhile, the EU combines the General Data Protection Regulation with national laws to regulate surveillance and data protection. Enacted in 2018, this regulatory framework sets stringent rules on data processing, granting individuals rights over their personal data and imposing obligations on entities that process such data. Each EU member state has its own laws governing surveillance, often requiring judicial authorisation for interception and establishing oversight bodies to monitor compliance. Data Protection Authorities in each member state oversee the enforcement of data protection laws, ensuring that surveillance activities comply with legal standards. The EU's approach accentuates the protection of individual rights and the necessity of oversight in surveillance activities.

India lacks these oversight mechanisms. The Pegasus case revealed that even when surveillance is conducted, there is no guaranteed pre-authorisation from an independent body or judiciary. Moreover, the government can claim "national security" as a shield. The

[9] Foreign Intelligence Surveillance Act 1978
[10] USA PATRIOT Act 2001

Supreme Court has recognised privacy as a fundamental right in the famous Puttaswamy case[11], but there is no statutory mechanism for citizens to challenge surveillance proactively.

Pegasus, as a spyware, operates without the victim's knowledge, potentially infecting devices silently by zero-click. Indian law does not specifically regulate spyware or zero-click exploits. Existing IT laws criminalise hacking, but government agencies often have exemptions. No legal clarity on what constitutes "legal government surveillance" vs illegal spyware deployment. The right to privacy is now recognised, but there is no clear legislation translating this right into enforceable procedural safeguards against digital surveillance. The government refuses to disclose the use of Pegasus, citing national security. No independent investigative authority can compel disclosure. Not to mention, citizens, journalists, and politicians have no effective remedies, leading to a chilling effect on free speech. If someone's privacy is violated, existing laws like the IT Act[12] or even the BNS[13] may allow filing a complaint, but in practice. Enforcement is poor as technical expertise is lacking in the lower courts. There are possibilities that victims cannot conclusively prove a spyware infection.

The findings of the committee founded by the Supreme Court have been met with criticism. The committee examined only 29 devices, a fraction of the potential targets. Moreover, the government reportedly did not cooperate fully with the investigation, hindering the committee's ability to obtain comprehensive data. Of the 29 devices analysed, only five were found to contain some form of malware. However, there was no conclusive evidence linking this malware to Pegasus spyware. The committee's final report was submitted in a sealed cover, limiting public access and transparency. Despite calls for disclosure, the Supreme Court has yet to release the full report, raising concerns about accountability. These issues clearly show the limited impact of the committee's work and question the effectiveness of such judicial commissions in addressing privacy and technological concerns. The Supreme Court has yet to deliver a final judgment on the matter. The case continues to be listed for hearings, but no conclusive decision has been made.

[11] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[12] Information Technology Act 2000
[13] Bharatiya Nyaya Sanhita 2023

CONCLUSION

The Pegasus controversy makes it clear that India's approach to privacy and surveillance is still incomplete. Privacy is now recognised as a fundamental right under the Constitution, but there is no proper law or procedure to protect it in practice. The Telegraph Act and the IT Act give the government wide powers to intercept or monitor communications, but these powers are vaguely defined and come with no independent oversight. There is no requirement for judicial authorisation, no monitoring body, and no clear distinction between lawful government surveillance and illegal spyware use.

The Supreme Court's response, i.e. forming a technical committee, looked like action on paper but fell short in practice. The committee examined only a handful of devices; the government did not fully cooperate, and the final report was submitted in a sealed cover. There was no transparency, no way to hold anyone accountable, and no real assurance that unauthorised surveillance could be stopped in the future. In effect, the Court tried to address the issue but ended up leaving the most important questions unanswered.

Until India has a comprehensive law governing digital surveillance, with clear procedures, independent oversight, and enforceable safeguards, the right to privacy remains vulnerable. The Pegasus case is not just about one spyware or one set of allegations; it is a test of whether constitutional rights can survive in the digital age. The state's power to monitor must be balanced against the individual's right to live without fear of intrusion, and until that balance is struck, privacy in India risks being more theoretical than real.