Spyware and Sovereignty

28 JULY 2025

Sixte Foucque and Lea Haupt



The Pegasus spyware scandal in Mexico has taken a new turn with revelations about former President Peña Nieto now under investigation for bribery. In July 2025, Mexican Attorney General Alejandro Gertz Manero announced an inquiry into allegations that former President Enrique Peña Nieto accepted up to $25 million in bribes from two Israeli businessmen linked to NSO Group, the company behind the infamous Pegasus spyware. This development follows the publication of an article in the Israeli newspaper The Marker, which claims that during his presidency, Peña Nieto received these payments from Avishai Neriah and Uri Ansbacher in exchange for facilitating lucrative contracts between Mexican government agencies and NSO Group. The former president denied the accusations first

on his X account and later in interviews, insisting he had no involvement in his government's contracting decisions.

Over the past decade, Pegasus has gained a reputation as one of the world's most notorious surveillance tools. Launched internationally in 2011 by the Israeli cyber firm NSO Group, Pegasus can hack virtually any mobile device—even if encrypted—and monitor all incoming and outgoing communications on both Android and iOS systems. Originally, its intrusion system was dependent on spear-fishing texts or emails (clicking on a malicious link); however, since 2016, NSO's improved intrusion capabilities claim to be capable of executing "zero-click" attacks. Usually via "zero-day" flaws within the operating system of the target. These attacks are also becoming increasingly efficient when they exploit weak points within apps that have nearly universal usage, such as WhatsApp or iMessages.

While marketed worldwide as a near-miraculous tool for tracking mafia bosses, terrorists, and other high-profile criminals, the software proved effective in the right hands; yet became hazardous when acquired by regimes eager to spy on political opponents, journalists, and activists. In 2021, the leak of a list containing some 50,000 phone numbers allegedly targeted by Pegasus revealed the alarming scale of its abuse. The Pegasus Project, a collaboration of 17 media outlets, used this leaked information to launch a major investigation revealing a large-scale misuse of Pegasus software by governments worldwide to hack into the phones of human rights activists, journalists, lawyers, and several heads of state. The French president, Nicolas Sarkozy, for example, was targeted by the Pegasus spyware.

In Mexico, Pegasus has been systematically misused to target journalists, activists, and political opponents. In 2011, under President Felipe Calderón, Mexico became the first country to purchase Pegasus spyware from Israel's NSO Group. At the time, the Mexican government was engaged in an intense fight against drug cartels and sought ways to break into their encrypted communications. While the U.S. National Security Agency (NSA) had developed methods to access these communications, it only granted Mexico limited access. Faced with this restriction, President Calderón saw Pegasus as an opportunity to develop an independent and advanced surveillance capability. Over the years, Mexico became NSO's most frequent customer. Although the software was originally acquired to target organised crime, its use soon expanded to surveil journalists, human rights defenders, and opposition figures. Among the most active users of Pegasus was the Mexican military, which, according to The New York Times, hacked more mobile phones than any other government agency worldwide. One of the best-known cases is that of journalist Carmen Aristegui, who had investigated corruption within the upper echelons of the Mexican government and whose phone was tapped using Pegasus during Enrique Peña Nieto's presidency.

The spyware has also been used to target some of the most prominent figures within Mexico's government. Alejandro Encinas, Mexico's under-

secretary for Human Rights, found, in 2018, the Pegasus spyware in his phone as well as that of two members of his office at a time when he was vividly criticizing the Mexican military and police force. For what he alleged was a cover-up after the disappearance of 43 students in Ayotzinapa in 2014. Thus raising the question of the military's involvement in the spying of former Mexican president Andrés Manuel López Obrador's top aides.

Given the Mexican government's documented history of using Pegasus to spy on journalists, lawyers, and human rights activists, these new revelations revive concerns about spyware misuse and the influence of tech companies at the highest levels of government. Mexico's current President, Claudia Sheibaum Pardo, has striven to continue the country's efforts towards militarisation and improved safety. Additionally, when asked about the use of spyware by her predecessor, she reiterated that the accusations were false, thereby reducing the likelihood that Pegasus will be stopped from being used by the current administration.

Mexico is certainly not the only North American nation faced with revelations of this kind. The United States District Court for the Northern District of California in the United States of America ordered in 2024 for the NSO group to hand over all materials connected to the Pegasus spyware after the NSO group was found guilty of attempting to hack into WhatsApp accounts over 1,400 times. Additionally, the Ontario Police Department in Canada acknowledged the use of a "growing ecosystem" of Israeli spyware to track down certain journalists. Canada's national police force has also been accused of, and has admitted to, using the spyware to access the data of civilian targets.