3 Main Points

Mexico's Attorney General is investigating former president Enrique Peña Nieto for accepting $25 million in bribes from Israeli businessmen for Pegasus spyware contracts.

Originally intended for criminal surveillance, Pegasus was widely abused in Mexico: agencies like the army used it to spy on journalists, activists, lawyers, and political opponents across multiple administrations.

Despite promises to reduce use, governance lapses persist, posing risks to democratic freedoms.

About the Authors

Lea is finishing her BA in Political and Social Studies at the University of Würzburg and will start a Master's in International Security at Sciences Po Paris in September. Her research focuses on transatlantic security and defense policy, with an interest in conflicts in India. She has work experience with the U.S. Embassy Berlin, German MoD, Bundestag, and a political risk consultancy. Lea also co-organizes a security policy academy with the Studienstiftung.

Sixte Foucque is a student of International Relations and Organisations at Leiden University. Having lived in the US, France, and Hong Kong, he has developed a keen interest in recent developments in the United States. This passion motivates his involvement with the North American Workgroup.

Dark Wings over Democracy

Sixte Foucque and Lea Haupt

This summer, 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 undersecretary 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 far from the only North American nation grappling with such revelations. In 2021, then-President Joe Biden blocked the NSO Group after determining that the Israeli firm's activities conflicted with American strategic interests and national security objectives. This federal restriction dealt a significant blow to the company while revealing deep U.S. concerns about the national defence risks posed by foreign surveillance technology.

The legal reckoning intensified in February 2024, when the U.S. District Court for the Northern District of California ordered NSO to provide its source code to WhatsApp as part of an ongoing lawsuit filed by Meta in 2019, following allegations by Meta that NSO's technology had been used to spy on over 1,400 WhatsApp users. In May 2025, a California federal jury delivered a

decisive verdict, ordering the Israeli surveillance company to pay $167.254 million in punitive damages for breaching approximately 1,400 WhatsApp accounts, plus an additional $444,719 in compensatory damages to Meta. This landmark decision represents a major victory against unlawful Pegasus deployment and establishes crucial legal precedent for future privacy violation cases.

Canada has also faced scrutiny over law enforcement spyware use. In 2022, the country's federal law enforcement agency acknowledged deploying sophisticated surveillance software against citizens in approximately ten cases between 2018 and 2020, prompting alarm among privacy experts who criticised Canada's inadequate oversight of such technology. More recently, in March 2025, Citizen Lab published a report alleging that Ontario Provincial Police had been using spyware called Graphite from Israeli company Paragon Solutions. These recurring revelations raise serious concerns about Canadian law enforcement's cyber-surveillance practices. Despite parliamentary calls for updated privacy legislation spanning over three years, no regulatory framework has been enacted to govern these activities.

Overall, the usage of spyware has greatly increased in the last decade, with the NSO group being the most advanced. Its “zero-click” capabilities make it a natural tool for technologically advanced states like Mexico, the United States, and Canada. Yet Mexico’s deployment of Pegasus goes beyond the bounds of legitimate surveillance, targeting journalists, human rights defenders, and political opponents in violation of constitutional protections. This misuse highlights the complex nature of these technologies, which exist in a murky space between legality, ethics, and unchecked power. As surveillance capabilities grow, so too must our vigilance. In a world where digital tools can silently undermine democracy, oversight is no longer optional; it is essential.


EPIS