Dutch MEP says illegal spyware ‘a grave threat to democracy’

Jennifer Rankin ⋮ 8-10 minutes ⋮ 11/8/2022

The senior MEP leading an inquiry into spyware has accused the EU commission of ignoring the “grave threat to democracy” posed by the use of the technology, and national governments of failing to cooperate with her investigation.

The Dutch liberal MEP Sophie in ‘t Veld said there was illegal use of spyware in Poland, Hungary, Greece and Spain and suspicions about Cyprus, while other EU member states made it easy for the “shady” industry to operate.

She accused national governments of failing to cooperate with her investigation, which is run by a European parliament special committee to look into the use of Pegasus – hacking software sold by the Israeli surveillance company NSO Group – and equivalent spyware in the wake of revelations from the Guardian and other media.

Publishing her interim report on Tuesday the MEP accused the European Commission, the body responsible for enforcing EU law, of silence in the face of a threat to democracy.

“The commission is very determined to fight attacks on democracy from the outside,” she said, citing its democracy action plan and response to Elon Musk’s takeover of Twitter. The EU’s internal market commissioner, Thierry Breton, had said on the platform that “in Europe, the bird [Twitter] will fly by our rules”.

The MEP added: “But … when the threat to democracy is not some far away stranger but the governments of EU member states, the commission suddenly considers that the defence of European democracy is no longer a European matter, but a matter for the member states. The commission shows muscle to Musk, but velvet gloves to member states using spyware on citizens.”

The European parliament’s Pegasus committee – the committee of inquiry investigating the use of Pegasus and equivalent surveillance spyware – was set up in March 2022 after 17 media outlets including the Guardian revealed the widespread use of hacking software by governments, including several EU member states.

The investigation was based on forensic analysis of phones and a leaked database of 50,000 numbers potentially of interest to clients of NSO, including that of the French president, Emmanuel Macron, the European Council president, Charles Michel, plus other officials, and opposition figures and journalists in 34 countries.

The spyware effectively turns people’s phones into surveillance devices without their knowledge, copying messages, harvesting photos and recording calls.

The MEP is calling for a ban on the sale, acquisition and use of spyware inside the EU unless member states can meet strict conditions guaranteeing appropriate use of the

technology. Conditions include ensuring there are investigations into alleged misuse of spyware, and having a legal framework in line with European human rights legislation.

To use the spyware EU member states would also be required to cooperate with Europol, and repeal export licences inconsistent with EU regulations aimed at controlling dangerous goods being sold to repressive regimes.

She acknowledged that any response would run into opposition from EU leaders and their ministers. The EU council of ministers has declined to answer questions from the Pegasus special committee about the use of spyware. A letter seen by the Guardian dated 12 October stated that oversight of EU law was the task of the commission, without providing responses to any questions.

“Some governments are abusing spyware, others are still behaving properly, but all of them use the cloak of national security to create an area of lawlessness,” in ‘t Veld said.

On Poland the report concluded that spyware was “an integral and vital part of a system designed specifically for the unfettered surveillance and control of citizens”.

Use of Pegasus in Poland first came to light in December 2021, after the Associated Press, with researchers at the Citizen Lab at the University of Toronto, reported that the technology had been used against at least three people, including Krzysztof Brejza, a Polish senator who was running the campaign of the opposition party Civic Platform.

In Hungary, about 300 people have been targeted, including political activists, journalists and a former government minister, according to the Hungarian media outlet Direkt 36, one of the media groups involved in the original investigation. The government in Budapest only confirmed last November it had acquired Pegasus spyware, after months of evasion.

In Greece there were signs that spyware was used in “a very systematic and large scale manner” the MEP said. Based on Greek media, her report said that at least 33 individuals had been targeted – “a stunning who’s who of politics, business and media”.

The Greek prime minister, Kyriakos Mitsotakis, has confirmed that the opposition leader Nikos Androulakis was targeted by spyware, which he described as a mistake that should never have happened. The report by in ‘t Veld states that Androulakis made an official complaint about an attempt to infect his phone with Predator spyware, a cheaper alternative to Pegasus.

Meanwhile in Spain, the report suggested there was a two-tier justice system, with the case of suspected spying on the prime minister, Pedro Sánchez, moving much faster than cases against the Spanish government brought by leaders of Catalonia’s independence movement. The phones of Sánchez, and those of his defence and interior ministers, are believed to have been hacked by Morocco’s government.

Morocco has denied spying on any foreign leaders using Pegasus, and has said reporters investigating NSO were “incapable of proving [the country had] any relationship” with that company.

The Catalan regional president, Pere Aragonès, said the report confirmed that the Spanish state had spied on dozens of pro-independence Catalan figures simply because

they had been, in his words, “working for the freedom of our country”.

The former Catalan president Carles Puigdemont, another apparent Pegasus target, said the report’s findings showed that Spain “spies and violates fundamental human rights”.

Puigdemont, who fled to Belgium to avoid arrest over his role in the illegal, unilateral, Catalan independence referendum held five years ago, said: “Mass, uncontrolled and illegal espionage is very serious, but it is even more so if it is carried out by a state and protected by the European Union.”

The report concluded that Cyprus was an “important European hub for the surveillance industry” casting doubt on Nicosia’s denials that the Israeli firm behind Pegasus, the NSO Group, had a subsidiary in the EU member state.

Bulgaria, Ireland, the Czech Republic and Luxembourg were named as countries facilitating the business of the spyware industry.

The MEP’s report, however, has yet to be endorsed by the other 37 members of the European parliament’s Pegasus committee. The chair of the committee, the Dutch centre-right MEP Jeroen Lenaers, distanced himself from the report by in ‘t Veld, saying her “first draft” should not be understood as the group’s conclusions. “Only the final report and recommendations, as adopted at the end of our period of activity, represents the position of the European parliament as a whole.”

The European Commission rejected the charge that it had been weak in the face of a threat to democracy. “The commission is always clear that any attempt by national security services to illegally access data of citizens, if confirmed, including journalists and politicians, political opponents, is unacceptable,” a spokesperson said. “Member states must oversee and control their security services to ensure that they fully respect fundamental rights, including the protection of personal data, safety of journalists and freedom of expression.”

The NSO Group has said it would take legal action against customers violating its agreements. “Once there is a suspicion that a customer misuses the technology sold by NSO, the company will investigate and will terminate the contract, if found to be true,” it said last December in response to similar allegations of government hacking.

The company announced in August it was appointing a new chief executive from inside the firm, as it promised to “ensure that the company’s groundbreaking technologies are used for rightful and worthy purposes”.

Additional reporting by Sam Jones in Madrid