SCHOLARLY ARTICLE

Tracing Surveillance Tools in Indonesia

Yakobus Dumupa

26 November 2026 · 54 min read

Abstrak

Nama Pegasus berulang kali disebut dalam perbincangan tentang penyadapan di Indonesia, tetapi jarang dibedakan antara yang terbukti dan yang diduga. Kajian kepustakaan ini menelusuri jejak alat penyadap di Indonesia melalui lima lapisan bukti: dokumen pengadaan, catatan pengiriman, infrastruktur internet, sasaran, dan proses hukum. Setiap klaim dinilai dengan skala keyakinan empat tingkat, lalu praktiknya diuji terhadap 13 Prinsip Kebutuhan dan Proporsionalitas dan terhadap syarat produsen serta negara pengekspor *spyware*. Pembelian sistem penyadapan tanpa klik oleh Polri sejak 2017 dan jejak sedikitnya lima vendor *spyware* dan alat pengawasan (Candiru, Wintego, Circles/Q Cyber, FinFisher, dan Predator) terdokumentasi kuat, sedangkan penggunaan Pegasus secara spesifik belum terbukti secara terbuka. Skandal yang terungkap pada November 2026 menunjukkan, menurut keterangan penyidik, bahwa sistem sadap resmi pun disalahgunakan untuk memantau Presiden, oposisi, aktivis, dan mahasiswa. Syarat produsen agar alat hanya dipakai untuk kejahatan serius dan sesuai hukum domestik tidak terlihat dipenuhi, antara lain karena Indonesia belum memiliki undang-undang penyadapan maupun aturan tentang *spyware*. Kajian ini merekomendasikan moratorium *spyware*, audit pengadaan, UU Penyadapan dengan izin dan pengawasan pengadilan, serta keikutsertaan dalam Proses Pall Mall.

Kata kunci: penyadapan, *spyware*, Pegasus, Polri, hak atas privasi, pengawasan negara

Abstract

The name Pegasus recurs in Indonesian debates on surveillance, yet proof and suspicion are rarely separated. This library-based study traces surveillance tools in Indonesia through five layers of evidence: procurement records, shipping records, internet infrastructure, targets, and legal proceedings. Each claim is graded on a four-level confidence scale, and practice is tested against the 13 Necessary and Proportionate Principles and the conditions set by spyware vendors and exporting states. Police purchases of zero-click interception systems since 2017 and traces of at least five spyware and surveillance vendors (Candiru, Wintego, Circles/Q Cyber, FinFisher, and Predator) are well documented, whereas the specific use of Pegasus has not been publicly proven. The scandal uncovered in November 2026 shows, according to investigators, that even official interception systems were abused to monitor the President, opposition figures, activists, and students. Vendor conditions that tools serve only serious crime and comply with domestic law do not appear to be met, partly because Indonesia has neither an interception law nor rules on spyware. The study recommends a spyware moratorium, procurement audits, an interception law with judicial authorization and oversight, and participation in the Pall Mall Process.

Keywords: interception, spyware, Pegasus, Indonesian National Police, right to privacy, state surveillance

1. Introduction

On 30 October 2026, several staff members of the monitoring unit at National Police Headquarters reported their own superiors to the Criminal Investigation Agency (Bareskrim). They had become suspicious after being ordered to disband a chat group and delete recordings and logs from the interception system. Four days later, Bareskrim named former National Police Chief General Listyo Sigit Prabowo, then serving as Presidential Chief of Staff, as a suspect and detained him (Tempo, 2026). According to the Police Chief's briefing to the House of Representatives (DPR), Listyo, who was Police Chief when the events took place, allegedly selected interception targets verbally or via WhatsApp and was the final recipient of the results. The targets included the President, ministries, members of the DPR, leaders of the Corruption Eradication Commission (KPK), prosecutors, activists, and students (CNN Indonesia, 2026).

Once the case broke, one name quickly filled the public sphere: Pegasus. Online media wrote of "traces of a surveillance weapon from Israel", and cyber experts speculated about zero-click attacks. The police themselves named only two systems, the Lawful Interception Management System (LIMS) and PenLink X, and have so far not mentioned Pegasus (Medcom, 2026). This pattern is not new. Since 2023, the name Pegasus has surfaced every time the issue of interception comes up, yet what is proven, what is merely suspected, and what is mistaken are rarely separated.

This vagueness harms two parties at once. For civil society, claims that cannot be proven are easily refuted and end up weakening demands for accountability. For the state, vagueness creates room to deny everything by denying a single name. Officials need only say "we do not use

Pegasus", while the more important questions remain unanswered: which surveillance tools were bought, from whom, on what legal basis, and used against whom.

This study seeks to untangle that vagueness in a simple way: by following the traces. Modern surveillance tools are designed to be invisible, but their procurement and use still leave marks in tender documents, customs records, internet servers, targets' phones, and case files. By sorting these traces one by one and assessing the strength of each, the study aims to answer four questions. First, which surveillance tools are proven to have entered Indonesia and to be held by state institutions? Second, what can and cannot be concluded about their use, including against critical groups? Third, does their use comply with the conditions set by vendors and exporting states, or does it deviate from them? Fourth, why has Indonesia's legal framework failed to control them, and what can be learned from other countries?

The literature on the global surveillance industry is already rich. Deibert (2020) describes how the same communication technologies that connect civil society have also become instruments of state espionage. Feldstein (2021) shows that states of diverse political character use digital technology to suppress dissent. The UN Special Rapporteur on freedom of expression, David Kaye, in 2019 described the private surveillance industry as a nearly uncontrolled field and called for a moratorium on the sale, transfer, and use of its tools until human rights-compliant safeguards were in place (Kaye, 2019). The call was repeated by the UN Office of the High Commissioner for Human Rights in 2022 (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2022). Penney (2016) provides empirical evidence that state surveillance causes people to restrict themselves in seeking information. In Indonesia, legal studies of interception are fairly numerous, especially on the KPK's powers and overlapping rules after Constitutional Court decisions (Hikmawati, 2022), but they generally focus on network interception, not *spyware*. Scholarly studies that combine all the evidence on *spyware* in Indonesia, from the 2023 investigations to the 2026 scandal, and test it against human rights standards and the vendors' own conditions, are still scarce. That is the contribution of this study.

2. Conceptual Framework

2.1 Interception, hacking, and spyware

The term "penyadapan" (interception) is used in Indonesian public debate for two activities that are in fact different. The first is the interception of communications through the network. Authorities ask telecommunications operators to forward calls and messages from particular numbers, usually through a lawful interception management system, or LIMS. This activity touches communications in transit, not the contents of the device, and leaves traces on the operator's side. The second is device intrusion. Authorities install spying software (*spyware*) on the target's phone so that its entire contents are exposed: messages in encrypted applications, photos, documents, location history, even the microphone and camera, which can be switched on remotely (Medcom, 2026; OHCHR, 2022).

The difference is not merely technical. Network interception can be regulated with the warrant and oversight models already familiar in criminal procedure law. Device intrusion is far more invasive because it not only intercepts ongoing communications but also opens up a person's entire life stored on the phone, including their past. The UN Office of the High Commissioner

for Human Rights places such hacking tools among the main threats to the right to privacy and calls for a moratorium on their sale, transfer, and use until a human rights-based safeguards regime exists (OHCHR, 2022). Amnesty International goes further, judging that highly invasive *spyware* such as Pegasus and Predator cannot possibly be used in a manner compatible with human rights (Amnesty International, 2024). This study therefore treats "surveillance tools" as an umbrella covering both, but always names the type, because that distinction determines the legal analysis.

Also worth noting is the term *zero-click*. It refers to the method of infection, namely that a phone can be compromised without the victim opening a link or taking any action. It is not the name of a product. Pegasus has this capability, but it is not the only one. Mistakenly equating *zero-click* with Pegasus is one source of the vagueness in the Indonesian debate.

2.2 Human rights benchmarks for interception

The right to privacy is not absolute. As summarised in the Academic Paper of the Interception Bill, the Constitutional Court regards privacy as a right that may be limited, but its limitation must be regulated by statute in accordance with Article 28J(2) of the 1945 Constitution (Dewan Perwakilan Rakyat Republik Indonesia, 2018). Article 17 of the International Covenant on Civil and Political Rights, ratified through Law No. 12 of 2005, prohibits arbitrary or unlawful interference with privacy and correspondence.

To translate that general principle into testable benchmarks, this study uses the *International Principles on the Application of Human Rights to Communications Surveillance*, known as the 13 Necessary and Proportionate Principles. The document was drafted through global consultation with civil society, industry, and experts, and is used as a framework for assessing whether surveillance laws are consistent with international human rights law (Necessary and Proportionate Coalition, 2014). The eight principles most relevant to this study are: legality (limitations are clearly set out in statute), legitimate aim (only for the most important state interests), necessity (the state must prove that surveillance is truly needed), proportionality (benefits are weighed against the harm to people's rights), competent judicial authority (decisions are taken by an independent judge), user notification (people under surveillance are notified with enough time and information to challenge it), transparency (the state discloses information on the use of surveillance powers), and public oversight (there is an independent oversight mechanism) (Necessary and Proportionate Coalition, 2014; Privacy International, 2013). These benchmarks are used in section 11 to assess Indonesia's legal framework.

2.3 Why surveillance is dangerous even when invisible

The danger of surveillance lies not only in the information stolen but also in the change in behaviour of people who feel watched. Penney (2016) provides some of the strongest empirical evidence for this. After the disclosure of the United States' mass surveillance programmes in June 2013, visits to Wikipedia articles on topics considered sensitive dropped significantly, and the decline persisted in the long term. This phenomenon is called the chilling effect: people restrict themselves, do not read, do not write, and do not speak, not because they are forbidden, but because they fear being watched.

The chilling effect explains why uncertainty about surveillance tools is as dangerous as proven abuse. When the public knows that the state buys phone-hacking tools but does not know who is targeted, every journalist, activist, lawyer, and opposition politician has reason to be careful. The vagueness itself becomes an instrument of control. This framework also explains why Kaye (2019) describes surveillance of journalists, activists, and opposition figures as a direct threat to freedom of expression, not merely a matter of privacy.

3. Method: Reading the Traces in Layers

3.1 Materials and approach

This study is library research using a normative juridical approach and analysis of secondary evidence. The author did not conduct forensic examinations or internet scanning himself. All technical findings come from institutions that publish their methodology openly, chiefly Amnesty International's Security Lab, the Citizen Lab at the University of Toronto, and Recorded Future's Insikt Group. Journalistic findings come from the IndonesiaLeaks consortium, Reuters, and national media. Official statements are taken from police statements, working meetings of DPR Commission III, and press releases of the relevant institutions. Legal materials include the 1945 Constitution, the Telecommunications Law, the State Intelligence Law, the Electronic Information and Transactions Law, sectoral laws containing interception powers, the new Criminal Procedure Code (KUHAP), National Police Chief Regulation No. 5 of 2010, and Constitutional Court Decisions No. 5/PUU-VIII/2010 and No. 70/PUU-XVII/2019. Non-legal materials include reports of the UN Special Rapporteur and the Office of the High Commissioner for Human Rights, policy documents of vendors and exporting states, and academic literature. Data were collected up to 25 November 2026.

3.2 Five layers of traces

The evidence is sorted into five layers according to where the traces are found. The first layer is procurement documents, namely tender packages and contracts in the government's electronic procurement system. The second layer is shipping records, namely cargo manifests and international trade data recording goods entering Indonesia. The third layer is internet infrastructure, namely servers and domain names whose fingerprints match particular *spyware* systems. The fourth layer is targets, namely warnings from phone manufacturers to users and the results of forensic examination of devices. The fifth layer is legal proceedings, namely investigators' statements and case documents.

This sorting matters because each layer proves something different. Procurement documents prove intent and budget, but not necessarily the product delivered. Shipping records prove that goods arrived, but often do not name the brand. Internet infrastructure proves that a system is operating, but rarely identifies its user. Evidence from targets proves an attack, but often cannot identify the attacker. Only legal proceedings have the potential to connect everything, and so far this has been the layer least often opened.

3.3 Confidence scale

Each claim is assessed on a four-level scale devised by the author with reference to the reporting practice of digital forensic research institutions, which commonly use expressions such as "high confidence" or "highly likely". The scale is shown in Table 1.

Table 1. Confidence scale used in this study

Level	Meaning	Minimum requirement
A. Proven	Fact can be verified from primary documents or official admission	Procurement documents, manifests, or official statements by investigators
B. Strong	Several independent pieces of evidence point to the same conclusion	Two layers of traces, or several independent sources within one layer, corroborating each other
C. Indicative	There are technical clues or source statements, but not yet confirmed by others	A single source in one layer of traces, or anonymous sources
D. Speculative	Suspicion without verifiable evidence	Opinion or mere similarity of pattern

Source: compiled by the author.

This method has limitations. The trade data used by Amnesty are incomplete and partly purchased from commercial databases. Many attributions rely on technical inference. Statements in the 2026 case have not yet been tested in court. The assessments in this study are therefore provisional and may change if new evidence emerges.

4. The First Layer: Traces in Procurement Documents

The earliest traces open to public scrutiny are in the electronic procurement system. The IndonesiaLeaks consortium, whose members include Tempo and several national media outlets and which works with OCCRP and Forbidden Stories, found that the Jakarta Metropolitan Regional Police (Polda Metro Jaya) and the National Police Intelligence and Security Agency (Baintelkam) procured a "zero click intrusion system", including a package titled the development of a zero-click intrusion system for iOS (Bisnis.com, 2023b; Tim IndonesiaLeaks, 2023).

The scale of procurement was large. In September 2017, Polda Metro Jaya bought a zero-click system upgrade worth Rp98 billion. In addition, there were records of a Wi-Fi data collection tool worth Rp99 billion, tactical vehicles worth Rp133 billion, a messaging application monitoring system worth Rp166 billion, and another zero-click system upgrade worth Rp149 billion. Over 2017–2021 there were eleven police interception equipment contracts, all won by a single company, PT Radika Karya Utama (Tim IndonesiaLeaks, 2023). Indonesia Corruption Watch verified the Rp98 billion 2017 package through the Opentender.net site and on 9 October 2023

went to National Police Headquarters to ask for its procurement documents to be disclosed (Kumparan, 2023). The request received no adequate answer (Bisnis.com, 2023a).

What do these traces mean? They prove that the police have long been buying the capability to break into phones without victim interaction, with budgets of hundreds of billions of rupiah. This claim stands at level A. But the tender documents do not name a brand. "*Zero-click*" is the name of a capability, not a product. Industry sources interviewed by IndonesiaLeaks equated the zero-click system with Pegasus, but a police official at the time, Inspector General Slamet Uliandi, denied it. According to him, zero-click tools had been in use since 2010 and did not necessarily mean Pegasus (Tim IndonesiaLeaks, 2023). The denial is not technically wrong, since several vendors sell similar capabilities. But it also does not answer which product was actually bought. Notably, three years later Slamet Uliandi, who headed the Police Information and Communication Technology Division when the events occurred, was himself named a suspect in the illegal interception scandal (CNN Indonesia, 2026).

The procurement traces also resurfaced in a DPR hearing. On 12 November 2026, Commission III member Ahmad Sahroni asked the police to show the physical existence of interception devices that had been bought in large numbers. He cited a figure of almost 300 units, adding "if I am not mistaken" (Katadata, 2026). The figure has not been verified, but the question shows that even the oversight body does not hold an inventory of police interception equipment.

5. The Second Layer: Traces in Shipping Records

The second layer is harder to hide because every incoming item passes through customs. IndonesiaLeaks found a shipment manifest in the name of PT Mandala Wangi Kreasindo, sent from London by Q Cyber Technologies, a company linked to NSO Group, the maker of Pegasus. The goods arrived at Soekarno-Hatta Airport on 1 December 2020. The manifest listed a Cisco router worth US$6,000 and a Dell server worth US$10,000, and a customs official confirmed the authenticity of the document. The company's office in Pasar Baru could not be found, its director declined to comment, and its shares had once been owned by the family of the wife of a minister in the Onward Indonesia Cabinet (Tim IndonesiaLeaks, 2023). Amnesty recorded the Q Cyber shipment to that Indonesian company with the date 15 December 2020; the difference in dates is probably due to the difference between the arrival date and the document date (Amnesty International, 2024).

Amnesty International's Security Lab, together with Haaretz, Tempo, Inside Story, WAV, and Woz, extended this inquiry through commercial trade databases. The result is a shipping map far broader than a single name. The Singaporean company Heha PTE Ltd sent hardware to the police on 20 May 2020, 3 July 2020, and 27 January 2021, with hardware worth around US$155,000 and declared software licences worth tens of millions of US dollars. The items matched the list in a leaked Candiru proposal, leading Amnesty to assess with high confidence that a Candiru system had been supplied, even though the shipping documents did not name Candiru (Amnesty International, 2024).

Other shipments were also recorded. ESW Systems, a Singaporean company, sent a Wintego-made "WINT SYSTEM" to the police on 9 September 2019 worth around US$5.6 million, and on

15 July 2021 sent a "watch list" detection licence worth around US$11 million along with real-time location tracking equipment. White Global Holdings sent an "Android one click installation module" to the treasurer of the National Cyber and Crypto Agency (BSSN) on 19 March 2019. Raedarius M8 Sdn Bhd of Malaysia, linked to FinFisher's parent company in Germany, sent hardware to PT Digital Solusi Prima on 7 August 2021 (Amnesty International, 2024). The makers of some shipments could not be identified.

The shipping pattern is consistent, and Figure 1 summarises it. Vendors in Israel or Europe do not sell directly, probably because Indonesia has no diplomatic relations with Israel and because direct routes are easy to trace. Goods and licences move through intermediary companies in Singapore, Malaysia, or Luxembourg, which often use nominee company secretaries so that the real owners are hard to identify. In Indonesia, local partner companies win tenders and then hand the systems over to state institutions (Amnesty International, 2024; Tim IndonesiaLeaks, 2023). According to IndonesiaLeaks sources, no more than ten companies hold NSO licences in Indonesia (Tim IndonesiaLeaks, 2023).

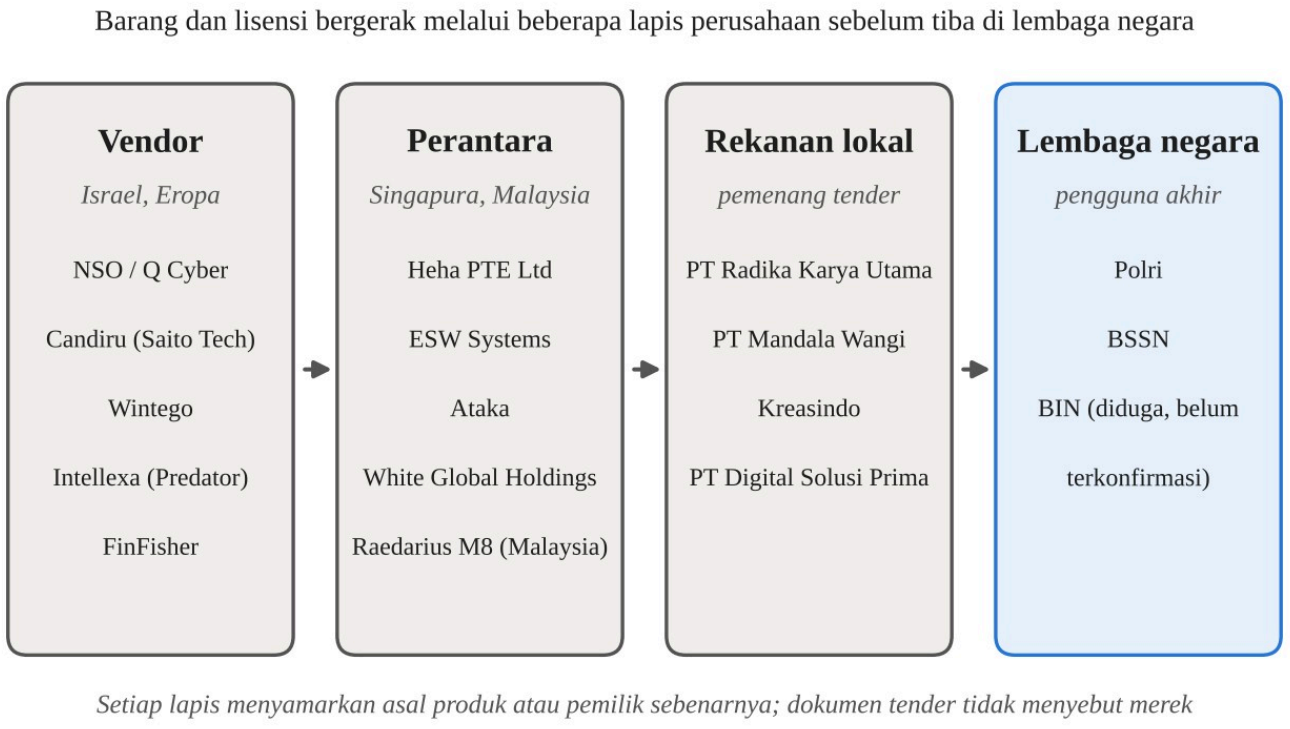


Figure 1. Procurement chain of interception tools and *spyware* to Indonesian state institutions

Source: compiled by the author based on Amnesty International (2024) and Tim IndonesiaLeaks (2023).

Layered chains like this hinder oversight from both directions. Exporting states find it hard to ascertain the end user, and the public in the importing country finds it hard to know what is bought with their taxes. Israel, for example, states that exports of cyber surveillance systems are granted only to government agencies for law enforcement and counter-terrorism, but does not publish its licensing information (Amnesty International, 2024).

6. The Third Layer: Traces on the Internet

Spyware needs infrastructure: servers to control infected phones and domain names for the bait links sent to targets. This infrastructure has technical fingerprints that can be recognised through internet scanning. It is in this layer that the evidence about Indonesia is most varied.

The oldest traces concern FinFisher. The Citizen Lab found FinSpy servers in Indonesia in 2013 and in 2015 linked them to the National Encryption Agency (Lembaga Sandi Negara), which later became BSSN. In 2018 Access Now also found a 2016 Indonesian Android application containing FinSpy and using the domain satgas.net. An IP address the domain had pointed to lay within a block linked to the National Counter-Terrorism Agency (BNPT), but the evidence is not sufficient to confirm BNPT as a customer (Amnesty International, 2024).

NSO traces in this layer do not take the form of Pegasus, but of Circles, an NSO affiliate that sells cellular network interception systems. A Circles surveillance system operated in an IP address block registered to "RADIKA KARTA UTAMA" from September 2018 until at least December 2020. Amnesty linked the name to PT Radika Karya Utama, the winner of the police interception tenders, although it found no company with exactly that name. Most importantly, Amnesty stated that it found no evidence that Pegasus itself had been installed by Radika (Amnesty International, 2024). This finding is consistent with a 2018 Citizen Lab report which, through internet scanning in 2016–2018, detected suspected Pegasus infections in 45 countries; Indonesia was not among them (Marczak et al., 2018). Indonesia's absence from that list does not prove that Pegasus was never used, but it shows that in that period no Indonesia-related Pegasus activity was detected by that method.

The Candiru traces are much clearer. In July 2021, the Citizen Lab and Microsoft exposed Candiru infrastructure in various countries and identified a customer system suspected to be in Indonesia (Marczak et al., 2021). Its domains, registered in November 2020, imitated IndoProgress, TribunNews, Tirto, Media Indonesia, and ANTARA. Up to 2022, domains appeared imitating the Gelora party with messages about relocating the capital, and domains imitating an Islamic charity (Amnesty International, 2024). Analysis by Insikt Group (2025) adds that one cluster of Candiru infrastructure very likely linked to a customer in Indonesia was still active until November 2024. Combined with the shipping records to the police in 2020–2021, the Candiru traces reach level B: two independent layers point to the same conclusion.

The traces of Predator, spyware made by the Intellexa consortium, have no shipping records, but its infrastructure was detected. A Predator backend server at an Indonesian IP address was first seen in December 2021 and was probably still active in December 2023. The earliest Indonesia-related bait domains, *ewestpapua.org* and *nindonesia.news*, were registered in March 2022. Other domains imitated a "Suara Oposisi" (Voice of the Opposition) site, the Suara Papua media outlet, and *geloraku.id*. According to Amnesty, these domains imitated opposition party sites as well as national and local media with a track record of documenting human rights violations (Amnesty International, 2024). In addition, Wintego left traces in the form of the domain *tribunnews.org*, imitating TribunNews, in August 2018, and a domain disguised as a Samsung update (Amnesty International, 2024).

The choice of domains offers a clue about the targets the operators had in mind. Links that look like news from Tirto, ANTARA, or opposition sites are most likely to be clicked by journalists, activists, politicians, and readers who follow political and human rights issues. But a clue is not proof. Amnesty itself stressed that it had no evidence that the technology had been used against particular members of civil society in Indonesia (Amnesty International, 2024). The claim that journalists, the opposition, and critical groups were the intended targets stands at level C.

7. The Fourth Layer: Traces on Targets' Phones

Traces on the target side are the scarcest, but one event stands out. In September 2022, Reuters reported that more than a dozen senior Indonesian government and military officials, including diplomats and advisers, had been targeted with spyware in 2021. Six of them said they had received emails from Apple in November 2021 stating that Apple believed they were being targeted by state-sponsored attackers (Potkin et al., 2022). Apple and security researchers said the tool used was ForcedEntry, a zero-click exploit previously used by NSO. A director of a state-owned enterprise supplying weapons to the Indonesian Army also received the same warning (Malay Mail, 2022).

This event is often cited as proof of Pegasus in Indonesia, though its conclusion is more limited. Reuters could not establish who made or used the spyware, whether the attacks succeeded, or what the attackers obtained. Another Israeli company, QuaDream, is known to have had an almost identical tool, and NSO denied involvement, calling it contractually and technologically impossible (Potkin et al., 2022). Because the targets were the state's own officials, the perpetrator could just as well have been a foreign intelligence service rather than a domestic agency. The targeting of Indonesian officials with NSO-class exploits stands at level B, while the identity of the attacker remains unknown.

Other claims from the target side are weaker. IndonesiaLeaks reported suspected monitoring of politicians ahead of the 2019 elections and of academics and activists in Yogyakarta and Bandung during the protests against the revision of the KPK Law, and said twelve senior government and military officials were suspected targets (Tim IndonesiaLeaks, 2023). Forensic results from the victims' phones have not been published, so this claim stands at level C. As of this writing, there is no public forensic report from the Citizen Lab, Amnesty, or Access Now confirming a Pegasus infection on an Indonesian citizen's phone.

The global context remains relevant. Apple sent a wave of mercenary spyware warnings to users in 110 countries in August 2026 and advised recipients to enable Lockdown Mode immediately and seek help from digital security experts (Bisnis.com, 2026). Apple did not say which countries were affected, so these data cannot be used to conclude anything about Indonesia specifically.

8. The Fifth Layer: Traces in Case Files

The November 2026 scandal opened a layer that had long been tightly closed. For the first time, the state's own investigators set out how interception tools were used outside the law.

According to the Head of Bareskrim, Commissioner General Asep Safrudin, the suspects allegedly ordered interceptions without following the procedures in National Police Chief Regulation No. 5 of 2010. A number of telephone numbers were entered into the LIMS server without an investigator's request letter or a warrant (Tempo, 2026). At a working meeting with DPR Commission III on 12 November 2026, Police Chief General Suyudi Ario Seto set out the chain of command. Target numbers were entered into LIMS without checking their link to any criminal case, then intercepted using the PenLink X (PLX) system. Recordings were listened to, exported, and transcribed. Listyo Sigit allegedly gave the orders and chose the targets; Inspector General Slamet Uliandi allegedly approved the interceptions and passed daily and analytical reports to Listyo; Inspectors General Eko Hadi Santoso and Ahrie Sonta, who alternately served as Acting Head of the Monitoring Section, allegedly passed the orders on to operators. In October 2026, Ahrie Sonta allegedly ordered the deletion of recordings and logs from LIMS and PLX, and it was this order that triggered the report by the monitoring staff (CNN Indonesia, 2026).

The categories of targets set out by the Police Chief were very broad: the President and Palace circles, ministries and agencies, DPR members and political parties, political figures, governors and regional police chiefs, the KPK, the Attorney General's Office, the police internally, community organisations, activists, and students (CNN Indonesia, 2026). The police have not announced how many numbers were intercepted (Tempo, 2026). Figures of "6,000" and "20,000 numbers" have circulated widely, including from a former official's social media posts (Sindonews, 2026b), but they have not been confirmed by investigators and therefore stand at level D. As of 24 November 2026, the number of suspects had grown to six from within the police, including Listyo Sigit, plus one civilian with the initials NE, and the case had expanded to alleged treason (Viva, 2026; Detik, 2026).

There are three lessons from this layer. First, according to investigators, the tools abused were not secret spyware but official interception systems lawfully purchased for law enforcement. Second, the abuse allegedly went on throughout 2025–2026 undetected by internal oversight, and was uncovered only because lower-level staff refused to delete evidence. Third, the targets were not limited to the elite. Activists, community organisations, and students were also monitored, something Amnesty International Indonesia considers potentially amounting to covert policing to tame the opposition, with victims who could number in the hundreds of activists, journalists, opposition politicians, and human rights defenders (Amnesty International Indonesia, 2026).

Was Pegasus involved in this scandal? Based on official statements, there is no evidence pointing that way. The police named LIMS and PLX and have not stated that Pegasus was present (Medcom, 2026). Some experts suspect a zero-click tool because LIMS cannot read the contents of encrypted applications (Suara, 2026), but this suspicion is not yet supported by data. A commentary writer in Antara also noted that the police have never stated that they bought Pegasus, although that suspicion cannot simply be dismissed (Wahyu S., 2026). The claim that the 2026 scandal used Pegasus stands at level D.

9. Weighing All the Traces

Figure 2 arranges all the traces discussed above by time and layer. It shows that the traces did not appear sporadically. Between 2017 and 2022, the first four layers were active almost simultaneously: tenders were opened, goods were shipped, servers were switched on, bait domains were registered, and officials received warnings. The fifth layer opened only in 2026. This pattern suggests a planned and sustained build-up of surveillance capability, not occasional purchases.

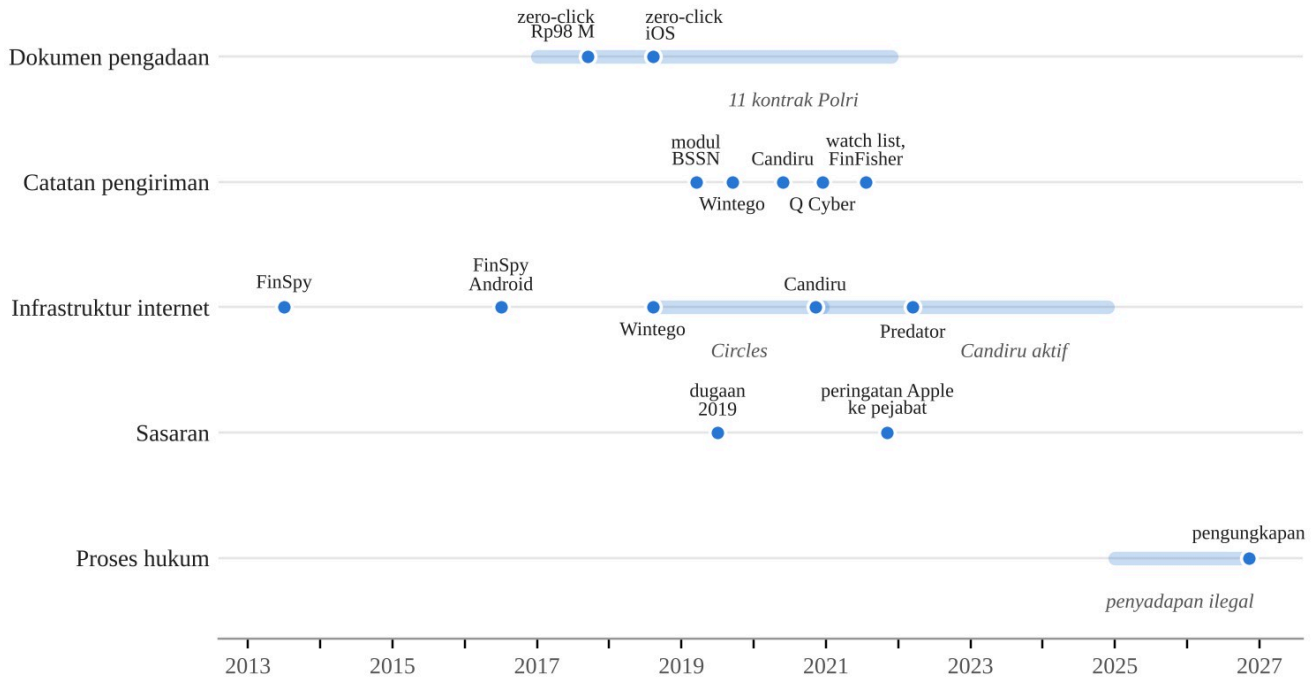


Figure 2. Traces of surveillance tools in Indonesia by layer of evidence, 2013–2026

Source: compiled by the author based on Amnesty International (2024), Tim IndonesiaLeaks (2023), Marczak et al. (2018, 2021), Insikt Group (2025), Potkin et al. (2022), and CNN Indonesia (2026).

Table 2 summarises the assessment of the main claims using the scale in Table 1.

Table 2. Assessment of the main claims about surveillance tools in Indonesia

Claim	Level	Basis of assessment
The police have bought zero-click interception systems since 2017 with budgets of hundreds of billions of rupiah	A	Electronic procurement documents; verified by ICW
Official police interception systems (LIMS and PLX) were abused to monitor the President, the opposition, activists, and students in 2025–2026	A†	Official statements by the Police Chief and Bareskrim; not yet tested in court
A Candiru system was supplied to the police and its infrastructure was active in Indonesia	B	Shipping records 2020–2021 and infrastructure 2020–2024 corroborate each other

Claim	Level	Basis of assessment
A Wintego system was supplied to the police	B	Shipping records 2019 and infrastructure 2018
Q Cyber/NSO equipment entered Indonesia and a Circles system operated	B	2020 manifest and IP traces 2018–2020
FinSpy operated in Indonesia and was attributed to the National Encryption Agency (now BSSN)	B	Citizen Lab scans 2013 and 2015; Access Now application sample 2018
Indonesian officials were attacked with an NSO-class exploit in 2021	B	Apple warnings to several officials; exploit identified by researchers; perpetrator unknown
Predator infrastructure was active in Indonesia	C	Server and domain scans; no shipping records; user unknown
News media and opposition sites were used as bait to target their readers	C	Pattern of bait domains; no verified victims yet
The police specifically use Pegasus	C	Anonymous sources; denied by the police; not confirmed by Amnesty
The 2026 interception scandal used Pegasus	D	Speculation; not supported by official statements

Source: author's analysis. †Level A for the existence of official investigators' statements; their material truth still awaits a court ruling.

From this assessment one conclusion can be drawn that is sharper than the public debate so far. The question "does Indonesia use Pegasus" turns out to be the wrong question. The evidence for Pegasus specifically is in fact the weakest, while the evidence for other equally invasive spyware, especially Candiru, is much stronger. As noted in section 2.1, Amnesty considers that spyware with such deep capabilities cannot possibly be used in a manner compatible with human rights. The issue, then, is not a particular brand, but the existence of phone-hacking capabilities in the hands of unsupervised institutions.

This assessment must also be read together with the structural limits of the evidence. Spyware is designed to go undetected, transactions take place through intermediaries, procurement documents are not disclosed, and victims rarely have their phones examined. A cyber observer quoted by Tempo even said that a tool that is easily detected is not a good tool (Tempo, 2023). The absence of forensic evidence is therefore not the same as evidence that spyware is not being used.

10. Does Its Use Comply with the Vendors' Rules?

10.1 Rules set by vendors and exporting states

Commercial spyware is not sold unconditionally, at least on paper. Vendors and exporting states set rules about who may buy and for what purposes the tools may be used. The question rarely asked in the Indonesian debate is whether those rules are observed.

NSO Group states that its technology is designed solely to prevent or investigate serious crime and terrorism, and that its customers, all of them government agencies, must agree to that condition as a condition of use (NSO Group, n.d.). In its first transparency report, NSO said every contract contains a human rights compliance clause and a customer commitment to use its systems only for the lawful prevention and investigation of serious crime and terrorism. The same report acknowledged that monitoring customers' activities remains a major challenge because NSO has no direct view of their use (Deccan Herald, 2021). NSO also says it reserves the right to suspend or terminate customers who do not comply with domestic laws and regulations, and says it has done so (NSO Group, 2020). According to its transparency reporting, NSO suspended or terminated six government customers in 2022–2023 and has cut off the systems of five customers since 2016 following misuse investigations (TechCrunch, 2026). Candiru, according to the Citizen Lab, sells spyware exclusively to governments (Marczak et al., 2021).

Exporting states add their own layer of rules. Israel approves exports of cyber systems only to government agencies for investigating and preventing terrorism and crime (Israel National News, 2021). On 6 December 2021, Israel's Defense Export Controls Agency (DECA) tightened the end-user declaration that buying states must sign. "Serious crime" was defined as an offence punishable by six years' imprisonment or more under the buying state's law, and expressing opinions or criticism, including about the state and its institutions, was affirmed as not in itself constituting a terrorist act (Janes, 2021). Violators of that commitment would immediately lose access to the systems they had bought (Jerusalem Post, 2021). A few weeks earlier, Israel had cut the list of countries allowed to buy offensive cyber products from 102 to 37, mostly Western European and English-speaking countries; Indonesia was not among them (Calcalist, 2021).

The United States took tougher steps against vendors. NSO Group and Candiru were added to the US Department of Commerce's Entity List in November 2021. Intellexa and Cytrox entities followed in July 2023, and the US Treasury sanctioned the founder and several entities of the Intellexa consortium in March 2024 (The Record, 2024b).

10.2 Testing practice in Indonesia

With those rules as the benchmark, Table 3 compares the conditions set by vendors and exporting states with documented practice in Indonesia.

Table 3. Rules of vendors and exporting states compared with practice in Indonesia

Rule	Documented practice in Indonesia	Assessment
The buyer must be a government agency	The end users are state institutions (police, BSSN), but goods were received and tenders won by private companies and brokers in third countries	Formally compliant, but the chain of intermediaries makes it hard for vendors to verify the end user
Only for serious crime and terrorism	Bait domains imitate media and opposition parties; suspected targeting of academics and activists in 2019; according to investigators, official interception systems were used against the President, the KPK, activists, and students with no link to any case in 2025–2026	Indications of deviation for *spyware*; for official interception systems, deviation revealed by investigators
Criticism and opinion are not terrorism (DECA, since December 2021)	Targets in 2025–2026 included community organisations, activists, and students	Contrary, if Israeli-made tools were also used; which tools were used is not yet proven
Must comply with domestic law	Indonesia has no interception law, and no law regulates device intrusion by the authorities	Almost impossible to meet; no domestic legal basis for the use of *spyware*
The buying state must be on the approved list (Israel, since November 2021)	Indonesia is not included; Candiru shipments are documented up to January 2021 and its infrastructure was still active until November 2024	Initial supply predated the tightening; status of later technical support unknown
The vendor may cut off customers who misuse the tools	No public information that any vendor has ever investigated or cut off a customer in Indonesia	The mechanism does not appear to work

Source: author's analysis based on NSO Group (n.d., 2020), Janes (2021), Calcalist (2021), Amnesty International (2024), Insikt Group (2025), and CNN Indonesia (2026).

The table shows that the easiest rule to meet, the government-buyer condition, is indeed formally met. But the conditions concerning the substance of use reveal a wide gap. The condition "only for serious crime and terrorism" is hard to believe is being observed when bait domains are designed to imitate news media and opposition parties, since such lures are better suited to reaching journalists, politicians, and activists than perpetrators of serious crime. The condition of compliance with domestic law is almost impossible to meet, since no law provides a basis for device intrusion by the authorities. In other words, the use of phone-hacking spyware by Indonesian state institutions can hardly be considered to meet the conditions set by its own vendors.

The 2026 scandal gives the clearest picture of deviation from legitimate purposes. The systems abused were indeed official interception systems, not Israeli spyware. But the pattern of deviation is exactly the pattern all vendor and exporter rules fear: targets chosen by WhatsApp message without any criminal case, including activists and students, with the results flowing to one person at the top of the hierarchy (CNN Indonesia, 2026). If a system bound by internal procedures and leaving traces at the operator can be abused in this way, there is no reason to assume that spyware which leaves no traces is treated more carefully.

There is also a question of timing. The shipments of equipment assessed by Amnesty as a Candiru system took place between May 2020 and January 2021, and the Wintego "watch list" licence was shipped in July 2021, all before Israel tightened its list of buying countries in November 2021 (Amnesty International, 2024; Calcalist, 2021). Yet Candiru infrastructure linked to a customer in Indonesia was reportedly still active until November 2024 (Insikt Group, 2025). Spyware of this kind usually requires regular exploit updates and technical support from its vendor. The available data do not allow a conclusion about whether such support continued after Indonesia dropped off Israel's export list, but the question deserves to be put to the Israeli government, the vendors, and the user institutions in Indonesia.

NSO's statement to Amnesty also needs careful reading. NSO stated that it does not provide active geolocation systems or phone-hacking systems to Indonesia based on its currently applicable due diligence procedures (Amnesty International, 2024). The phrase "currently applicable" does not answer the question about the period before those procedures were applied, does not cover its affiliate Circles, whose system was recorded operating in Indonesia in 2018–2020, and does not explain the equipment shipment from Q Cyber in December 2020.

Finally, the safeguard mechanisms promised by vendors do not appear to work in Indonesia. NSO itself admits it has no direct view of how its systems are used, while Candiru declined to discuss its licences, citing legal reasons (Amnesty International, 2024). There is no public information that any vendor has ever investigated or cut off a customer in Indonesia. Vendor rules thus function more as reputational protection for sellers than as protection for the people under surveillance. Real control can only come from law and oversight bodies in the user country, and that is where Indonesia is weakest.

11. Why the Law Fails to Exercise Control

11.1 A mandate not carried out

The Constitution guarantees the right to security and personal protection in Article 28G(1) and the right to communicate in Article 28F of the 1945 Constitution. These guarantees are reinforced by Article 17 of the ratified International Covenant on Civil and Political Rights (see section 2.2). Interception is a limitation of rights, so under Article 28J(2) of the 1945 Constitution it may only be carried out on the basis of statute.

The Constitutional Court has affirmed this. In Decision No. 5/PUU-VIII/2010, read out on 24 February 2011, the Court annulled Article 31(4) of the Electronic Information and Transactions Law, which left interception procedures to a government regulation, and affirmed that interception must be regulated by statute (Putusan MK Nomor 5/PUU-VIII/2010). Fifteen years later,

that statute still does not exist. The new Criminal Procedure Code, Law No. 20 of 2025, in force since 2 January 2026, merely defines interception and leaves its regulation to a special law. Conditions, duration, judicial authorisation mechanisms, storage, and destruction of intercepted material remain unregulated (Hukumonline, 2026).

11.2 Fragmented rules

In this vacuum, interception powers are scattered across various laws with differing conditions. The Telecommunications Law in principle prohibits interception in Article 40, then provides an exception in Article 42(2): for the purposes of criminal justice, operators may record and provide information at the written request of the Attorney General and/or the National Police Chief for certain offences, or at the request of investigators in accordance with applicable law (Hukumonline, 2009). Sectoral laws then regulate the powers of each institution, as summarised in Table 4.

Table 4. Interception powers under sectoral laws

Institution	Legal basis	Authorisation	Duration
KPK	Law 19/2019 Articles 12 and 12C in conjunction with Constitutional Court Decision 70/PUU-XVII/2019	No warrant; accountable to the leadership and notified to the Supervisory Board no later than 14 working days after completion	No longer regulated since Article 12B was annulled
Narcotics investigators	Law 35/2009 Articles 77–78	Written permission of the chief of the district court; in urgent cases, permission sought no later than 1×24 hours afterwards	3 months, extendable once
Terrorism investigators	Law 15/2003 in conjunction with Law 5/2018 Articles 31–31A	Written permission of the chief of the district court; in urgent cases, notification no later than 3 days afterwards	1 year, extendable once
Human trafficking investigators	Law 21/2007 Article 31	Written permission of the chief of the court	At most 1 year
BIN	Law 17/2011 Articles 31–32	Order of the Head of BIN; determination by the chief of the district court if the target already has sufficient preliminary evidence	6 months, extendable as needed
Police (general)	Law 36/1999 Article 42(2); Police Chief Regulation 5/2010	Written request of the Police Chief or investigators; internal procedures	Regulated internally

Institution	Legal basis	Authorisation	Duration
Prosecutors	Law 11/2021 Article 30C letter i	Dependent on a special interception law that does not yet exist	Not yet regulated

Source: compiled from the relevant laws, Constitutional Court Decision No. 70/PUU-XVII/2019, Detik (2021), Hikmawati (2022), Hukumonline (2009, 2017), and Saidin (2026).

The table shows inconsistency in two respects. In terms of authorisation, some institutions must seek court permission, some need only notify an internal supervisor, and some rely solely on internal procedures. In terms of time, interception periods vary from three months to one year with possible extensions, or even without clear limits (Saidin, 2026). For the KPK, the six-month limit also fell when the Court annulled Article 12B in its entirety (Putusan MK Nomor 70/PUU-XVII/2019). Hikmawati (2022) notes that this inconsistency creates legal uncertainty, and that even the Court's decision on the KPK has not fulfilled the Court's earlier call for a special law designating the authorising authority. The police, the institution that buys the most interception equipment, work on the weakest basis, namely National Police Chief Regulation No. 5 of 2010, which according to the Indonesian Legal Aid Foundation (YLBHI) is no longer in step with legal developments and the mandate of the Court's decisions (Kontan, n.d.). The State Intelligence Law places interception under the order of the Head of the State Intelligence Agency (BIN) and requires a court determination only when the target already has sufficient preliminary evidence (Detik, 2021), and experts judged from the outset that its mechanism and authorisation were not strictly regulated (Hukumonline, 2012).

Measured against the 13 Necessary and Proportionate Principles, the result is clear. The principle of legality is not met for the police, because their interception procedures are regulated only in an internal regulation, not in a statute as ordered by the Constitutional Court. The principle of judicial authority is met only partly, for certain offences. The principle of user notification is unknown in any law: there is no obligation to notify people who have been intercepted, even after a case is closed. The principles of transparency and public oversight are not met either, because there are no periodic reports on the number of interceptions and procurement documents are closed. As a result, the principles of legitimate aim, necessity, and proportionality cannot be meaningfully tested: without a judge or independent body examining the reasons for each interception before it is carried out, no one weighs whether the interception is necessary and proportionate to the harm to the rights of the person intercepted.

The 2026 scandal shows the consequences. Internal police procedures require an investigator's request letter, but that requirement could be bypassed by a verbal order or a WhatsApp message from the top leadership. No judge gave permission before the interception, no outside party checked the list of numbers, and there was no periodic audit of the system logs. The safeguard that finally worked seems to have been nothing more than the conscience of a few staff members who refused to erase the traces.

11.3 Spyware: a field with no rules at all

If interception through operators is not well regulated, spyware lies in an even darker field. Indonesia has no law regulating the lawful use of spyware and surveillance technology (Al Jazeera, 2024). The difference matters both technically and legally. LIMS works through telecommunications operators' networks and at least leaves traces on the operator's side. Spyware such as Pegasus or Candiru works by breaking into the phone itself, so it does not pass through the operator at all and can read the contents of encrypted applications, photos, and documents, and switch on the microphone and camera (Medcom, 2026). Intrusion of this kind is more accurately called hacking than interception.

The Electronic Information and Transactions Law criminalises illegal access to electronic systems (Article 30) and illegal interception (Article 31). Article 31 does exempt interception by law enforcement, but only when carried out on the basis of statute. Because no statute regulates device intrusion by the authorities, that exemption is hard to apply. When state institutions do it, what takes place is hacking by the state without legal cover.

11.4 Blunt oversight of procurement

The last gap concerns procurement. Tender documents for interception equipment are treated as secret, so the public and even the DPR do not know what is being bought (Bisnis.com, 2023a). ICW's 2023 request went without an adequate answer, and in response to Amnesty's 2024 report, the police received the letter but declined to answer questions, while BSSN did not respond (Amnesty International, 2024). The DPR only asked about the physical existence of police interception equipment after the 2026 scandal broke (Katadata, 2026). Oversight that moves only after a scandal resembles firefighting more than oversight.

12. Learning from Other Countries

Indonesia is not the only country facing a spyware scandal, and the experience of other countries shows the paths that can be taken once a scandal is exposed.

Poland offers the most relevant example. The new government formed at the end of 2023 disclosed the previous government's use of Pegasus. Prosecutor General Adam Bodnar reported to parliament that Pegasus had been used against 578 people in 2017–2022 by three agencies, namely the Central Anti-Corruption Bureau, the Military Counterintelligence Service, and the Internal Security Agency (Associated Press, 2024). Parliament set up a special commission of inquiry, and prosecutors summoned victims for questioning. A Citizen Lab researcher described the Polish government's disclosure of victim data as the first in the European Union (The Record, 2024a). The process was not smooth, as the Polish Constitutional Tribunal, whose independence has been questioned, declared the commission unconstitutional, but the commission continued its work (Notes from Poland, 2024).

At the European Union level, the European Parliament set up the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA). The committee concluded that spyware had been used to violate fundamental rights and endanger democracy in several member states, with Poland and Hungary as the most glaring cases (European

Parliament, 2023). On 15 June 2023, the European Parliament adopted reform recommendations and specifically called on Poland, Hungary, Greece, Spain, and Cyprus to follow up on the violations that had occurred (Eucrim, 2023). In Greece, it was confirmed that a Member of the European Parliament and a journalist had been wiretapped by the intelligence service and targeted with Predator spyware (Parliamentary Assembly of the Council of Europe, 2023).

At the global level, multilateral initiatives have begun to take shape. The Pall Mall Process, launched by the United Kingdom and France in February 2024, produced a Code of Practice for States in April 2025. The code is voluntary and non-binding, but sets out good practice for states in developing, facilitating, purchasing, transferring, and using commercial cyber intrusion capabilities (UK Government, 2025). It rests on four pillars: accountability, precision, transparency, and oversight (CyberScoop, 2025). Its initial signatories were mostly European states, plus Japan and Ghana, and Indonesia was not among them (YesWeHack, 2025).

Three lessons can be drawn for Indonesia. First, a scandal can become a turning point if it is followed by full disclosure: the number of victims, the user institutions, and the legal basis for each interception, as Poland did. Second, parliamentary inquiry is effective only if oversight bodies remain independent; the European Parliament noted that in Poland and Hungary, the dismantling of independent oversight mechanisms was itself the root of the abuse (European Parliament, 2023). Third, Indonesia can use international frameworks such as the Pall Mall Code of Practice as a benchmark for drafting its own law, without having to start from scratch.

13. Conclusions and Recommendations

13.1 Conclusions

Tracing the five layers of evidence and testing them against human rights standards and vendor conditions yields four conclusions, which also answer the study's four questions.

First, Indonesia has a large, layered, and closed ecosystem of surveillance tools. The police have bought zero-click interception systems since 2017 with budgets of hundreds of billions of rupiah, and products from at least five spyware and surveillance vendors, namely Candiru, Wintego, Circles/Q Cyber, FinFisher, and Predator, left traces in Indonesia between 2013 and 2024. These goods entered through networks of intermediaries in Singapore, Malaysia, and Luxembourg that disguised their origin and destination.

Second, the specific use of Pegasus by Indonesian state institutions has not been publicly proven. The evidence for Pegasus is in fact the weakest compared with the evidence for other equally invasive spyware. Public focus on a single brand has obscured the larger problem and made denial easier.

Third, the 2025–2026 interception scandal, according to official investigators' statements not yet tested in court, shows that official interception systems can be widely abused to monitor the President, state institutions, the opposition, activists, community organisations, and students without being detected by internal oversight. If systems that leave traces at the operator can be abused this widely, the risk from spyware that leaves no traces is far greater.

Fourth, the root of the problem is a vacuum of law and oversight, so that neither human rights standards nor vendor conditions can be enforced. Fifteen years after the Constitutional Court's decision, Indonesia still has no interception law, has no rules on spyware, and does not disclose procurement documents for interception equipment. Bait domains imitating news media and opposition sites show that journalists, the opposition, and critical groups are the most vulnerable in this vacuum. The conditions set by vendors and exporting states do not fill that vacuum: the serious-crime condition does not appear to be met, the domestic-law compliance condition is almost impossible to meet, and the customer cut-off mechanism does not appear to work.

13.2 Recommendations

1. The government should impose a moratorium on the purchase and use of phone-hacking spyware by all state institutions until a law regulates it in line with human rights standards, consistent with the calls of the UN Special Rapporteur (Kaye, 2019), the UN Office of the High Commissioner for Human Rights (OHCHR, 2022), and Amnesty International Indonesia (2026).
2. The DPR and the government should draft an Interception Law that harmonises the powers of all institutions, requires judicial authorisation before interception, limits the duration and types of offences, regulates the storage and destruction of intercepted material, and requires notification of the people intercepted after the interception ends where it no longer endangers the investigation. The law must regulate spyware separately and far more strictly than interception through operators, or prohibit it altogether.
3. Deliberation of the Interception Bill, resumed in November 2026 (Sindonews, 2026a), should be conducted openly and involve civil society, so that the sense of emergency after the scandal does not instead produce a law legalising broad interception powers.
4. The Supreme Audit Agency (BPK) and independent oversight bodies should audit all procurement of interception equipment and spyware by the police, BSSN, BIN, and other institutions since 2017, including its physical existence, operational status, and usage logs. The audit results should be reported to the DPR in a forum that is publicly accountable.
5. The investigation of the 2026 scandal must not stop at the dimensions of state security and alleged treason. The police should disclose the number of victims, their categories, and the basis of each interception, as Poland did. Victims among activists, journalists, community organisations, and students should be notified, given access to the data collected about them, and receive remedy. The establishment of an independent committee involving civil society, as proposed by Amnesty International Indonesia (2026), deserves consideration.
6. The government should request official explanations from exporting states and vendors about export licences, end users, and technical support for systems supplied to Indonesia, and should declare its participation in the Pall Mall Process and make its Code of Practice the benchmark for drafting legislation.
7. Institutions authorised to intercept should publish annual transparency reports on the number of requests, authorisations, and interceptions carried out, in line with the principles of transparency and public oversight in the 13 Necessary and Proportionate Principles.

8. Civil society, especially human rights organisations, journalists, lawyers, and advocacy groups, should strengthen their digital security capacity: regular device updates, Lockdown Mode for those at high risk, vigilance towards links imitating media, and forensic examination through the Access Now Digital Security Helpline or Amnesty's Security Lab when there is suspicion. Collective documentation of suspected attacks is the evidence that has been most lacking in the Indonesian case.

This inquiry began with a question about a single name, but ends with a more fundamental problem. What needs to be traced is no longer merely the trail of Pegasus, but the trail of accountability: who buys, who uses, who oversees, and who protects the citizens under surveillance. As long as those questions cannot be answered from official documents, citizens are forced to seek the answers themselves from cargo manifests, internet servers, and the courage of a handful of staff who refused to delete the evidence.

References

Al Jazeera. (2024, 3 May). *Israeli firms sold invasive surveillance tech to Indonesia: Report*. https://www.aljazeera.com/news/2024/5/3/israeli-firms-sold-invasive-surveillance-tech-to-indonesia-report

Amnesty International. (2024, 2 May). *A web of surveillance: Unravelling a murky network of spyware exports to Indonesia* (ASA 21/7974/2024). https://securitylab.amnesty.org/latest/2024/05/a-web-of-surveillance/

Amnesty International Indonesia. (2026, 4 November). *Skandal penyadapan bukan semata-mata soal Presiden, ini soal oposisi yang dijinakkan* [Press release]. https://www.amnesty.id/kabar-terbaru/siaran-pers/skandal-penyadapan-bukan-semata-soal-presiden-ini-soal-oposisi-yang-dijinakkan/11/2026/

Associated Press. (2024, 24 April). *Poland's prosecutor general says previous government used spyware against hundreds of people*. Courthouse News Service. https://www.courthousenews.com/polands-prosecutor-general-says-previous-government-used-spyware-against-hundreds-of-people/

Bisnis.com. (2023a, 9 October). *ICW desak Polri buka-bukaan soal alat sadap asal Israel "Pegasus"*. https://kabar24.bisnis.com/read/20231009/16/1702458/icw-desak-polri-buka-bukaan-soal-alat-sadap-asal-israel-pegasus

Bisnis.com. (2023b, 12 June). *Mengenal zero click, alat spionase senyap diduga beredar di RI*. https://kabar24.bisnis.com/read/20230612/16/1664460/mengenal-zero-click-alat-spionase-senyap-diduga-beredar-di-ri

Bisnis.com. (2026, 19 August). *Pengguna iPhone di 110 negara jadi target spyware, Apple kirimkan notifikasi*. https://teknologi.bisnis.com/read/20260819/280/1997420/pengguna-iphone-di-110-negara-jadi-target-spyware-apple-kirimkan-notifikasi

Calcalist. (2021, 25 November). *Israel defense ministry slashes cyber export list, drops Saudi Arabia, UAE*. https://www.calcalistech.com/ctech/articles/0,7340,L-3923361,00.htm

CNN Indonesia. (2026, 13 November). *Fakta-fakta baru kasus penyadapan Prabowo oleh Listyo Sigit dkk*. https://www.cnnindonesia.com/nasional/20261113071349-12-1426643/fakta-fakta-baru-kasus-penyadapan-prabowo-oleh-listyo-sigit-dkk

CyberScoop. (2025). *Voluntary Pall Mall Process seeks to curb spyware abuses*. https://cyberscoop.com/voluntary-pall-mall-process-seeks-to-curb-spyware-abuses/

Deccan Herald. (2021). *NSO Group flagged misuse risk of its spyware before Pegasus row erupted*. https://www.deccanherald.com/amp/national/nso-group-flagged-misuse-risk-of-its-spyware-before-pegasus-row-erupted-1011415.html

Deibert, R. J. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi Press.

Detik. (2021). *Kejaksaan bisa menyadap, ini bedanya dengan KPK*. https://news.detik.com/berita/d-5847464/kejaksaan-bisa-menyadap-ini-bedanya-dengan-kpk

Detik. (2026, 24 November). *Bareskrim tetapkan 1 tersangka sipil di kasus penyadapan oleh Listyo cs*. https://news.detik.com/berita/d-8767303/bareskrim-tetapkan-1-tersangka-sipil-di-kasus-penyadapan-oleh-listyo-cs

Dewan Perwakilan Rakyat Republik Indonesia. (2018). *Naskah akademik Rancangan Undang-Undang tentang Penyadapan*. https://berkas.dpr.go.id/puupolhukham/na/file/na-19.doc

Eucrim. (2023, 31 July). *EP recommendation on lessons learned from misused spyware*. https://eucrim.eu/news/ep-recommendation-on-lessons-learned-from-misused-spyware/

European Parliament. (2023, 9 May). *Spyware: MEPs sound alarm on threat to democracy and demand reforms* [Press release]. https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Hikmawati, P. (2022). Pengaturan izin penyadapan oleh KPK pasca Putusan Mahkamah Konstitusi No. 70/PUU-XVII/2019. *Negara Hukum, 13*(1), 83–102. https://dprexternal3.dpr.go.id/index.php/hukum/article/download/2969/pdf

Hukumonline. (2009). *Penyadapan*. https://www.hukumonline.com/berita/a/penyadapan-lt4b34d3deb69c6/

Hukumonline. (2012). *Ahli: UU Intelijen mengandung kelemahan*. https://www.hukumonline.com/berita/a/ahli--uu-intelijen-mengandung-kelemahan-lt4f86be11e105f/

Hukumonline. (2017). *Disepakati, penyadapan harus mendapat izin pengadilan*. https://www.hukumonline.com/berita/a/disepakati--penyadapan-harus-mendapat-izin-pengadilan-lt59786898d8d1f/

Hukumonline. (2026). *Penyadapan dan penggeledahan data digital dalam KUHAP baru*. https://www.hukumonline.com/klinik/a/penyadapan-dan-penggeledahan-data-digital-dalam-kuhap-baru-lt508a387a44f53

Insikt Group. (2025). *[Cyber threat analysis of Candiru spyware infrastructure]* (CTA-2025-0805). Recorded Future. https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf

Israel National News. (2021, 6 December). *Defense Ministry tightens control of cyber exports*. https://www.israelnationalnews.com/news/318201

Janes. (2021, 7 December). *Israel tightens regulations around cyber exports*. https://www.janes.com/defence-news/news-detail/israel-tightens-regulations-around-cyber-exports

Jerusalem Post. (2021, 7 December). *Defense Ministry to tighten regulation on cyber exports*. https://www.jpost.com/breaking-news/defense-ministry-to-tighten-regulation-on-cyber-exports-687998

Katadata. (2026, 12 November). *Sahroni pertanyakan keberadaan ratusan alat sadap Polri*. https://katadata.co.id/amp/berita/nasional/6af52c0554a17/sahroni-pertanyakan-keberadaan-ratusan-alat-sadap-polri

Kaye, D. (2019). *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/41/35). United Nations Human Rights Council. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_35.docx

Kontan. (n.d.). *YLBHI desak DPR segera bentuk UU Penyadapan*. https://nasional.kontan.co.id/news/ylbhi-desak-dpr-segera-bentuk-uu-penyadapan

Kumparan. (2023, 9 October). *ICW dkk desak Polri transparan buka data pengadaan alat sadap Pegasus*. https://kumparan.com/kumparannews/icw-dkk-desak-polri-transparan-buka-data-pengadaan-alat-sadap-pegasus-21Lb0ybh6TH

Malay Mail. (2022, 30 September). *Senior Indonesian officials targeted by spyware last year, say sources*. https://www.malaymail.com/news/world/2022/09/30/senior-indonesian-officials-targeted-by-spyware-last-year-say-sources/30882

Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., & Deibert, R. (2021). *Hooking Candiru: Another mercenary spyware vendor comes into focus* (Citizen Lab Research Report No. 139). University of Toronto. https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). *Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries* (Citizen Lab Research Report No. 113). University of Toronto. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Medcom. (2026). *LIMS di penyadapan Prabowo dan Pegasus: Bedanya sistem penyadapan jaringan dan spyware ponsel*. https://www.medcom.id/teknologi/news-teknologi/PNg1RZ9k-lims-di-penyadapan-prabowo-dan-pegasus-bedanya-sistem-penyadapan-jaringan-dan-spyware-ponsel

Necessary and Proportionate Coalition. (2014). *International principles on the application of human rights to communications surveillance*. https://necessaryandproportionate.org/13-principles

Notes from Poland. (2024, 10 September). *Poland's constitutional court finds commission investigating use of Pegasus spyware unconstitutional*. https://notesfrompoland.com/2024/09/10/polands-constitutional-court-finds-commission-investigating-use-of-pegasus-spyware-unconstitutional/

NSO Group. (n.d.). *NSO Group reply* [Response to Business & Human Rights Resource Centre]. https://www.business-humanrights.org/documents/5269/NSO_Group_reply.pdf

NSO Group. (2020, 2 June). *Response from NSO Group*. Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/response-from-nso-group

Office of the United Nations High Commissioner for Human Rights [OHCHR]. (2022). *The right to privacy in the digital age* (A/HRC/51/17). United Nations. https://digitallibrary.un.org/record/3985679

Parliamentary Assembly of the Council of Europe. (2023). *Pegasus and similar spyware and secret state surveillance* (Doc. 15825). https://pace.coe.int/en/files/33018/html

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117–182. https://doi.org/10.15779/Z38SS13

Potkin, F., Allard, T., Lamb, K., & Bing, C. (2022, 30 September). *Senior Indonesian officials targeted by spyware last year*. Al Jazeera (from Reuters). https://www.aljazeera.com/economy/2022/9/30/indonesian-officials-targeted-by-spyware-sources

Privacy International. (2013). *Introducing the International Principles on the Application of Human Rights to Communications Surveillance*. https://privacyinternational.org/blog/1191/introducing-international-principles-application-human-rights-communications-surveillance

Saidin, O. K. (2026). *Penyadapan dan ujian negara hukum*. Kumparan. https://kumparan.com/ok-saidin/penyadapan-dan-ujian-negara-hukum-28WcWopCc2D

Sindonews. (2026a, 16 November). *Cegah kasus Listyo Sigit terulang, Komisi III DPR mulai bahas RUU Penyadapan*. https://nasional.sindonews.com/read/1772663/13/cegah-kasus-listyo-sigit-terulang-komisi-iii-dpr-mulai-bahas-ruu-penyadapan-1794813083

Sindonews. (2026b, 9 November). *Said Didu ungkap 20.000 nomor HP dalam 4 kelompok disadap tim LSP*. RCTI+. https://rctiplus.com/news/detail/nasional/5512460/said-didu-ungkap-20-000-nomor-hp-dalam-4-kelompok-disadap-tim-lsp

Suara. (2026, 13 November). *Prabowo diduga disadap pakai Pegasus, pakar soroti potensi keterlibatan asing*. https://www.suara.com/news/2026/11/13/220336/prabowo-diduga-disadap-pakai-pegasus-pakar-soroti-potensi-keterlibatan-asing

TechCrunch. (2026). *NSO Group releases new transparency report*. https://techcrunch.com/?p=3080919

Tempo. (2023, 19 June). *Soal spyware Pegasus, kenapa pengamat siber ini angkat tangan?* https://tekno.tempo.co/read/1738740/soal-spyware-pegasus-kenapa-pengamat-siber-ini-angkat-tangan

Tempo. (2026, 4 November). *Modus penyadapan ilegal yang menjerat Listyo Sigit Prabowo*. https://www.tempo.co/hukum/penyadapan-ilegal-yang-menjerat-listyo-sigit-2303398

The Record. (2024a). *Over 500 people targeted by Pegasus spyware in Poland, officials say*. https://therecord.media/poland-pegasus-spyware-more-than-500-citizens

The Record. (2024b, 5 Maret). *US sanctions Predator spyware makers for targeting government officials*. https://therecord.media/predator-spyware-makers-sanctioned-for-targeting-government-officials

Tim IndonesiaLeaks. (2023, 12 June). *Kepak Pegasus di Indonesia*. Tempo. https://interaktif.tempo.co/proyek/kepak-pegasus-di-indonesia/

UK Government. (2025). *The Pall Mall Process Code of Practice for States*. https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states

Viva. (2026, 24 November). *Round up: Kasus penyadapan ilegal berujung makar, Listyo Sigit dan 5 polisi jadi tersangka*. https://www.viva.co.id/berita/nasional/1945902-round-up-kasus-penyadapan-ilegal-berujung-makar-listyo-sigit-dan-5-polisi-jadi-tersangka

Wahyu S., B. (2026, 12 November). *Bayang-bayang Pegasus dalam isu penyadapan Presiden*. Antara. https://www.antaranews.com/berita/5848815/bayang-bayang-pegasus-dalam-isu-penyadapan-presiden

YesWeHack. (2025, 10 April). *Spyware pact draws distinction between malicious and legitimate use of cyber-intrusion tools*. https://www.yeswehack.com/news/spyware-pact-malicious-legitimate-use

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang.

Undang-Undang Nomor 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights.

Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.

Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang.

Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan Kedua atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi.

Undang-Undang Nomor 11 Tahun 2021 tentang Perubahan atas Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.

Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 5 Tahun 2010 tentang Tata Cara Penyadapan pada Pusat Pemantauan Kepolisian Negara Republik Indonesia.

Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 tentang Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Putusan Mahkamah Konstitusi Nomor 70/PUU-XVII/2019 tentang Pengujian Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan Kedua atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi.

HOW TO CITE

Dumupa, Y. (2026). Tracing surveillance tools in Indonesia [Scholarly article]. Yakobus Dumupa. https://yakobusdumupa.com/kajian/mencari-jejak-alat-penyadap-di-indonesia?lang=en