KAJIAN ILMIAH

Mencari Jejak Alat Penyadap di Indonesia

Yakobus Dumupa

26 November 2026

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

Daftar Isi

1. Pendahuluan....3
2. Kerangka Konseptual....4
2.1 Penyadapan, peretasan, dan spyware....4
2.2 Ukuran hak asasi manusia untuk penyadapan....4
2.3 Mengapa pengawasan berbahaya meski tidak terlihat....5
3. Metode: Membaca Jejak Secara Bertingkat....5
3.1 Bahan dan pendekatan....5
3.2 Lima lapisan jejak....6
3.3 Skala keyakinan....6
4. Lapisan Pertama: Jejak di Dokumen Pengadaan....7
5. Lapisan Kedua: Jejak di Catatan Pengiriman....7
6. Lapisan Ketiga: Jejak di Internet....9
7. Lapisan Keempat: Jejak di Ponsel Sasaran....10
8. Lapisan Kelima: Jejak di Berkas Perkara....11
9. Menimbang Seluruh Jejak....12
10. Apakah Penggunaannya Sesuai Aturan Produsen?....14
10.1 Aturan yang dibuat produsen dan negara pengekspor....14
10.2 Menguji praktik di Indonesia....14
11. Mengapa Hukum Tidak Mampu Mengendalikan....16
11.1 Mandat yang tidak dilaksanakan....16
11.2 Aturan yang terpecah-pecah....17
11.3 Spyware: wilayah tanpa aturan sama sekali....18
11.4 Pengawasan pengadaan yang tumpul....18
12. Belajar dari Negara Lain....19
13. Simpulan dan Rekomendasi....20
13.1 Simpulan....20
13.2 Rekomendasi....20
Daftar Pustaka....21

1. Pendahuluan

Pada 30 Oktober 2026, sejumlah staf bagian pemantauan di Mabes Polri melaporkan atasan mereka sendiri ke Bareskrim. Mereka curiga karena diperintahkan membubarkan grup percakapan dan menghapus rekaman serta log dari sistem penyadapan. Empat hari kemudian, Bareskrim menetapkan mantan Kapolri Jenderal Listyo Sigit Prabowo, yang saat itu menjabat Kepala Staf Kepresidenan, sebagai tersangka dan menahannya (Tempo, 2026). Menurut paparan Kapolri di DPR, Listyo, yang menjabat Kapolri ketika peristiwa itu terjadi, diduga menentukan sasaran penyadapan secara lisan atau melalui WhatsApp dan menjadi penerima akhir hasilnya. Sasarannya mencakup Presiden, kementerian, anggota DPR, pimpinan KPK, kejaksaan, aktivis, dan mahasiswa (CNN Indonesia, 2026).

Begitu kasus itu terbuka, satu nama segera memenuhi ruang publik: Pegasus. Media daring menulis tentang “jejak senjata intai dari Israel”, dan pakar siber berspekulasi tentang serangan tanpa klik. Polri sendiri hanya menyebut dua sistem, yaitu *Lawful Interception Management System* (LIMS) dan PenLink X, dan sejauh ini tidak menyebut Pegasus (Medcom, 2026). Pola seperti ini bukan hal baru. Sejak 2023, nama Pegasus selalu muncul setiap kali isu penyadapan mencuat, tetapi jarang dipisahkan mana yang terbukti, mana yang sekadar diduga, dan mana yang keliru.

Kekaburan itu merugikan dua pihak sekaligus. Bagi masyarakat sipil, tuduhan yang tidak bisa dibuktikan mudah dibantah dan akhirnya melemahkan tuntutan akuntabilitas. Bagi negara, kekaburan memberi ruang untuk menyangkal segalanya dengan menyangkal satu nama. Pejabat cukup berkata “kami tidak memakai Pegasus”, sementara pertanyaan yang lebih penting tidak terjawab: alat penyadap apa saja yang dibeli, dari siapa, dengan dasar hukum apa, dan dipakai terhadap siapa.

Kajian ini berupaya mengurai kekaburan itu dengan cara yang sederhana: menelusuri jejak. Alat penyadap modern dirancang untuk tidak terlihat, tetapi pengadaan dan penggunaannya tetap meninggalkan bekas di dokumen tender, catatan kepabeanan, server di internet, ponsel sasaran, dan berkas perkara. Dengan memilah jejak-jejak itu satu per satu dan menilai kekuatan masing-masing, kajian ini hendak menjawab empat pertanyaan. Pertama, alat penyadap apa saja yang terbukti masuk ke Indonesia dan dimiliki lembaga negara? Kedua, apa yang dapat dan tidak dapat disimpulkan tentang penggunaannya, termasuk terhadap kelompok kritis? Ketiga, apakah penggunaannya sesuai dengan syarat yang ditetapkan produsen dan negara pengekspor, atau justru menyimpang? Keempat, mengapa kerangka hukum Indonesia gagal mengendalikannya, dan apa yang dapat dipelajari dari negara lain?

Literatur tentang industri pengawasan global sudah cukup kaya. Deibert (2020) menggambarkan bagaimana teknologi komunikasi yang sama yang menghubungkan masyarakat sipil juga menjadi sarana pengintaian oleh negara. Feldstein (2021) menunjukkan bahwa negara-negara dengan beragam corak politik memakai teknologi digital untuk menekan perbedaan pendapat. Pelapor Khusus PBB untuk kebebasan berekspresi, David Kaye, pada 2019 menyebut industri pengawasan swasta sebagai wilayah yang nyaris tanpa kendali dan menyerukan moratorium penjualan, pengalihan, dan penggunaan alat-alatnya sampai ada kerangka pengaman yang sesuai hak asasi manusia (Kaye, 2019). Seruan itu diulang Kantor Komisaris Tinggi HAM PBB pada 2022 (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2022). Penney (2016) memberikan bukti empiris bahwa pengawasan negara membuat orang membatasi diri dalam mencari informasi. Di Indonesia, kajian hukum

tentang penyadapan cukup banyak, terutama tentang kewenangan KPK dan tumpang-tindih aturan setelah putusan Mahkamah Konstitusi (Hikmawati, 2022), tetapi umumnya berfokus pada penyadapan melalui jaringan, bukan *spyware*. Kajian ilmiah yang memadukan seluruh bukti tentang *spyware* di Indonesia, dari investigasi 2023 sampai skandal 2026, dan mengujinya terhadap standar hak asasi manusia serta syarat produsennya sendiri, belum banyak ditemukan. Di situlah kontribusi kajian ini.

2. Kerangka Konseptual

2.1 Penyadapan, peretasan, dan spyware

Istilah "penyadapan" dalam perbincangan publik di Indonesia dipakai untuk dua kegiatan yang sebenarnya berbeda. Yang pertama adalah intersepsi komunikasi melalui jaringan. Aparat meminta operator telekomunikasi meneruskan percakapan dan pesan dari nomor tertentu, biasanya melalui sistem manajemen intersepsi sah atau LIMS. Kegiatan ini menyentuh komunikasi yang sedang lewat, bukan isi perangkat, dan meninggalkan jejak di sisi operator. Yang kedua adalah pembobolan perangkat. Aparat memasang perangkat lunak mata-mata (*spyware*) ke dalam ponsel sasaran sehingga seluruh isinya terbuka: pesan di aplikasi terenkripsi, foto, dokumen, riwayat lokasi, bahkan mikrofon dan kamera yang bisa dinyalakan dari jauh (Medcom, 2026; OHCHR, 2022).

Perbedaan ini bukan soal teknis semata. Intersepsi melalui jaringan dapat diatur dengan model izin dan pengawasan yang sudah dikenal dalam hukum acara pidana. Pembobolan perangkat jauh lebih invasif karena tidak hanya menyadap komunikasi yang sedang berlangsung, tetapi juga membuka seluruh kehidupan seseorang yang tersimpan di ponsel, termasuk masa lalunya. Kantor Komisaris Tinggi HAM PBB menempatkan alat peretasan semacam ini sebagai salah satu ancaman utama terhadap hak atas privasi dan menyerukan moratorium penjualan, pengalihan, dan penggunaannya sampai ada rezim pengaman berbasis hak asasi manusia (OHCHR, 2022). Amnesty International bahkan menilai *spyware* yang sangat invasif, seperti Pegasus dan Predator, penggunaannya tidak mungkin dibuat sesuai dengan hak asasi manusia (Amnesty International, 2024). Karena itu, kajian ini memperlakukan "alat penyadap" sebagai payung yang mencakup keduanya, tetapi selalu menyebut jenisnya, karena pembedaan itulah yang menentukan analisis hukumnya.

Yang juga perlu dicatat adalah istilah *zero-click* atau "tanpa klik". Istilah ini menunjuk pada cara infeksi, yaitu ponsel dapat dibobol tanpa korban membuka tautan atau melakukan tindakan apa pun. Ia bukan nama produk. Pegasus memiliki kemampuan ini, tetapi bukan satu-satunya. Kekeliruan menyamakan *zero-click* dengan Pegasus menjadi salah satu sumber kekaburan dalam perdebatan di Indonesia.

2.2 Ukuran hak asasi manusia untuk penyadapan

Hak atas privasi tidak mutlak. Sebagaimana dirangkum dalam Naskah Akademik RUU Penyadapan, Mahkamah Konstitusi memandang privasi sebagai hak yang dapat dibatasi, tetapi pembatasannya harus diatur dengan undang-undang sesuai Pasal 28J ayat (2) UUD 1945 (Dewan Perwakilan Rakyat Republik Indonesia, 2018). Pasal 17 Kovenan Internasional tentang Hak-Hak Sipil dan Politik, yang diratifikasi melalui UU Nomor 12 Tahun 2005, melarang campur tangan yang sewenang-wenang atau tidak sah terhadap urusan pribadi dan korespondensi.

Untuk menerjemahkan prinsip umum itu ke dalam ukuran yang dapat diuji, kajian ini memakai *Prinsip-Prinsip Internasional tentang Penerapan Hak Asasi Manusia terhadap Pengawasan Komunikasi*, yang dikenal sebagai 13 Prinsip Kebutuhan dan Proporsionalitas. Dokumen ini disusun melalui konsultasi global dengan masyarakat sipil, industri, dan pakar, dan dipakai sebagai kerangka untuk menilai apakah hukum pengawasan sejalan dengan hukum HAM internasional (Necessary and Proportionate Coalition, 2014). Delapan prinsip paling relevan untuk kajian ini adalah: **legalitas** (pembatasan diatur jelas dalam undang-undang), **tujuan sah** (hanya untuk kepentingan negara yang paling penting), **kebutuhan** (negara wajib membuktikan bahwa pengawasan benar-benar perlu), **proporsionalitas** (manfaat ditimbang terhadap kerugian bagi hak orang), **otoritas peradilan yang berwenang** (keputusan diambil oleh hakim yang independen), **pemberitahuan kepada pengguna** (orang yang disadap diberi tahu dengan cukup waktu dan informasi untuk menggugat), **transparansi** (negara membuka informasi tentang penggunaan kewenangan pengawasan), dan **pengawasan publik** (ada mekanisme pengawasan yang independen) (Necessary and Proportionate Coalition, 2014; Privacy International, 2013). Ukuran inilah yang dipakai pada bagian 11 untuk menilai kerangka hukum Indonesia.

2.3 Mengapa pengawasan berbahaya meski tidak terlihat

Bahaya pengawasan tidak hanya terletak pada informasi yang dicuri, tetapi juga pada perubahan perilaku orang yang merasa diawasi. Penney (2016) memberikan salah satu bukti empiris paling kuat tentang hal ini. Setelah pengungkapan program pengawasan massal Amerika Serikat pada Juni 2013, kunjungan ke artikel Wikipedia tentang topik yang dianggap sensitif turun secara signifikan, dan penurunan itu bertahan dalam jangka panjang. Gejala ini disebut efek gentar (*chilling effect*): orang membatasi diri, tidak membaca, tidak menulis, dan tidak berbicara, bukan karena dilarang, tetapi karena takut diawasi.

Efek gentar menjelaskan mengapa ketidakpastian tentang alat penyadap sama berbahayanya dengan penyalahgunaan yang terbukti. Ketika publik tahu bahwa negara membeli alat pembobol ponsel tetapi tidak tahu siapa yang menjadi sasaran, setiap jurnalis, aktivis, pengacara, dan politisi oposisi punya alasan untuk berhati-hati. Kekaburan itu sendiri menjadi alat kontrol. Kerangka ini juga menjelaskan mengapa Kaye (2019) menyebut pengawasan terhadap jurnalis, aktivis, dan tokoh oposisi sebagai ancaman langsung terhadap kebebasan berekspresi, bukan sekadar persoalan privasi.

3. Metode: Membaca Jejak Secara Bertingkat

3.1 Bahan dan pendekatan

Kajian ini merupakan penelitian kepustakaan dengan pendekatan yuridis-normatif dan analisis bukti sekunder. Penulis tidak melakukan pemeriksaan forensik atau pemindaian internet sendiri. Seluruh temuan teknis berasal dari lembaga yang menerbitkan metodologinya secara terbuka, terutama Amnesty International Security Lab, Citizen Lab di Universitas Toronto, dan Insikt Group dari Recorded Future. Temuan jurnalistik berasal dari konsorsium IndonesiaLeaks, Reuters, dan media nasional. Keterangan resmi diambil dari pernyataan Polri, rapat kerja Komisi III DPR, dan siaran pers lembaga terkait. Bahan hukum mencakup UUD 1945, UU Telekomunikasi, UU Intelijen Negara, UU Informasi dan Transaksi Elektronik, undang-undang sektoral yang memuat kewenangan penyadapan, KUHAP baru, Peraturan Kapolri Nomor 5 Tahun 2010, serta Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010

dan Nomor 70/PUU-XVII/2019. Bahan nonhukum mencakup laporan Pelapor Khusus dan Kantor Komisaris Tinggi HAM PBB, dokumen kebijakan produsen dan negara pengekspor, serta literatur akademik. Data dihimpun sampai 25 November 2026.

3.2 Lima lapisan jejak

Bukti dipilah ke dalam lima lapisan menurut tempat jejak itu ditemukan. Lapisan pertama adalah **dokumen pengadaan**, yaitu paket tender dan kontrak di sistem pengadaan elektronik pemerintah. Lapisan kedua adalah **catatan pengiriman**, yaitu manifes kargo dan data dagang internasional yang mencatat barang masuk ke Indonesia. Lapisan ketiga adalah **infrastruktur internet**, yaitu server dan nama domain yang sidik jarinya cocok dengan sistem *spyware* tertentu. Lapisan keempat adalah **sasaran**, yaitu peringatan dari produsen ponsel kepada pengguna dan hasil pemeriksaan forensik perangkat. Lapisan kelima adalah **proses hukum**, yaitu keterangan penyidik dan dokumen perkara.

Pemilahan ini penting karena setiap lapisan membuktikan hal yang berbeda. Dokumen pengadaan membuktikan niat dan anggaran, tetapi belum tentu produk yang dikirim. Catatan pengiriman membuktikan barang tiba, tetapi sering tidak menyebut merek. Infrastruktur internet membuktikan sistem beroperasi, tetapi jarang menunjuk pemakainya. Bukti dari sasaran membuktikan serangan, tetapi sering tidak dapat menunjuk penyerangnya. Hanya proses hukum yang berpotensi menyambungkan semuanya, dan selama ini lapisan inilah yang paling jarang terbuka.

3.3 Skala keyakinan

Setiap klaim dinilai dengan skala empat tingkat yang disusun penulis dengan mengacu pada praktik pelaporan lembaga riset forensik digital, yang lazim memakai ungkapan “keyakinan tinggi” atau “kemungkinan besar”. Skala itu ditunjukkan dalam Tabel 1.

Tabel 1. Skala keyakinan yang dipakai dalam kajian ini

Tingkat	Arti	Syarat minimum
A. Terbukti	Fakta dapat diverifikasi dari dokumen primer atau pengakuan resmi	Dokumen pengadaan, manifes, atau keterangan resmi penyidik
B. Kuat	Beberapa bukti independen menunjuk ke kesimpulan yang sama	Dua lapisan jejak, atau beberapa sumber independen dalam satu lapisan, saling menguatkan
C. Indikatif	Ada petunjuk teknis atau keterangan narasumber, tetapi belum dikonfirmasi pihak lain	Satu sumber dalam satu lapisan jejak, atau sumber anonim
D. Spekulatif	Dugaan tanpa bukti yang dapat diperiksa	Opini atau kemiripan pola semata

Sumber: disusun penulis.

Metode ini memiliki keterbatasan. Data dagang yang dipakai Amnesty tidak lengkap dan sebagian dibeli dari basis data komersial. Banyak atribusi bergantung pada inferensi teknis. Keterangan dalam perkara 2026 belum diuji di pengadilan. Karena itu, penilaian dalam kajian ini bersifat sementara dan dapat berubah bila bukti baru muncul.

4. Lapisan Pertama: Jejak di Dokumen Pengadaan

Jejak paling awal yang dapat diperiksa publik terdapat di sistem pengadaan elektronik. Konsorsium IndonesiaLeaks, yang beranggotakan Tempo dan sejumlah media nasional serta bekerja sama dengan OCCRP dan Forbidden Stories, menemukan bahwa Polda Metro Jaya dan Badan Intelijen dan Keamanan (Baintelkam) Polri melakukan pengadaan "zero click intrusion system", termasuk paket berjudul pengembangan sistem intrusi tanpa klik untuk iOS (Bisnis.com, 2023b; Tim IndonesiaLeaks, 2023).

Skala pengadaannya besar. Pada September 2017, Polda Metro Jaya membeli peningkatan sistem tanpa klik senilai Rp98 miliar. Di luar itu tercatat alat pengumpul data Wi-Fi senilai Rp99 miliar, mobil taktis Rp133 miliar, sistem pemantau aplikasi pesan Rp166 miliar, dan satu lagi peningkatan sistem tanpa klik Rp149 miliar. Sepanjang 2017–2021 terdapat sebelas kontrak alat sadap Polri, dan semuanya dimenangkan oleh satu perusahaan, PT Radika Karya Utama (Tim IndonesiaLeaks, 2023). Indonesia Corruption Watch memverifikasi paket 2017 senilai Rp98 miliar melalui situs Opentender.net dan pada 9 Oktober 2023 mendatangi Mabes Polri untuk meminta dokumen pengadaannya dibuka (Kumparan, 2023). Permintaan itu tidak mendapat jawaban yang memadai (Bisnis.com, 2023a).

Apa arti jejak ini? Ia membuktikan bahwa Polri sudah lama membeli kemampuan membobol ponsel tanpa interaksi korban, dengan anggaran ratusan miliar rupiah. Klaim ini berada pada tingkat A. Namun dokumen tender tidak menyebut merek. Istilah "*zero-click*" adalah nama kemampuan, bukan nama produk. Narasumber industri yang ditemui IndonesiaLeaks menyamakan sistem tanpa klik dengan Pegasus, tetapi pejabat Polri saat itu, Irjen Slamet Uliandi, membantah. Menurutnya, alat tanpa klik sudah dipakai sejak 2010 dan tidak selalu berarti Pegasus (Tim IndonesiaLeaks, 2023). Bantahan itu secara teknis tidak salah, karena beberapa vendor menjual kemampuan serupa. Tetapi bantahan itu juga tidak menjawab produk apa yang sebenarnya dibeli. Patut dicatat, tiga tahun kemudian Slamet Uliandi, yang menjabat Kadiv TIK Polri ketika peristiwa itu terjadi, justru ditetapkan sebagai tersangka dalam skandal penyadapan ilegal (CNN Indonesia, 2026).

Jejak pengadaan juga muncul kembali dalam rapat DPR. Pada 12 November 2026, anggota Komisi III Ahmad Sahroni meminta Polri menunjukkan keberadaan fisik alat sadap yang pernah dibeli dalam jumlah besar. Ia menyebut angka hampir 300 unit, dengan catatan "kalau tidak salah" (Katadata, 2026). Angka itu belum diverifikasi, tetapi pertanyaannya menunjukkan bahwa lembaga pengawas pun tidak memegang inventaris alat sadap kepolisian.

5. Lapisan Kedua: Jejak di Catatan Pengiriman

Lapisan kedua lebih sulit disembunyikan karena setiap barang yang masuk melewati kepabeanan. IndonesiaLeaks menemukan manifes kiriman atas nama PT Mandala Wangi Kreasindo, yang dikirim dari London oleh Q Cyber Technologies, perusahaan yang terkait dengan NSO Group, pembuat Pegasus. Barang itu tiba di Bandara Soekarno-Hatta pada 1 Desember 2020. Manifes mencantumkan sebuah router Cisco senilai US$6.000 dan server Dell senilai US$10.000, dan seorang pejabat bea cukai membenarkan keaslian dokumennya. Kantor perusahaan itu di Pasar Baru tidak dapat ditemukan, direkturnya menolak berkomentar, dan sahamnya pernah dimiliki keluarga istri seorang menteri Kabinet Indonesia Maju (Tim IndonesiaLeaks, 2023). Amnesty mencatat kiriman Q Cyber ke perusahaan Indonesia itu

dengan tanggal 15 Desember 2020; perbedaan tanggal kemungkinan disebabkan perbedaan antara tanggal tiba dan tanggal dokumen (Amnesty International, 2024).

Amnesty International Security Lab, bersama Haaretz, Tempo, Inside Story, WAV, dan Woz, memperluas penelusuran ini melalui basis data perdagangan komersial. Hasilnya adalah peta pengiriman yang jauh lebih luas daripada satu nama. Perusahaan Singapura Heha PTE Ltd mengirim perangkat keras ke Polri pada 20 Mei 2020, 3 Juli 2020, dan 27 Januari 2021, dengan nilai perangkat keras sekitar US$155.000 dan lisensi perangkat lunak yang dideklarasikan bernilai puluhan juta dolar AS. Barang-barang itu cocok dengan daftar dalam proposal Candiru yang pernah bocor, sehingga Amnesty menilai dengan keyakinan tinggi bahwa sistem Candiru telah dipasok, meskipun dokumen kiriman tidak menyebut nama Candiru (Amnesty International, 2024).

Kiriman lain juga tercatat. ESW Systems, perusahaan Singapura, mengirim “WINT SYSTEM” buatan Wintego ke Polri pada 9 September 2019 dengan nilai sekitar US$5,6 juta, dan pada 15 Juli 2021 mengirim lisensi deteksi “watch list” senilai sekitar US$11 juta beserta perangkat pelacak lokasi seketika. White Global Holdings mengirim “Android one click installation module” kepada bendahara BSSN pada 19 Maret 2019. Raedarius M8 Sdn Bhd dari Malaysia, yang terhubung dengan induk FinFisher di Jerman, mengirim perangkat keras ke PT Digital Solusi Prima pada 7 Agustus 2021 (Amnesty International, 2024). Produsen beberapa kiriman tidak dapat diidentifikasi.

Pola pengirimannya konsisten, dan Gambar 1 merangkumnya. Vendor di Israel atau Eropa tidak menjual langsung, kemungkinan karena Indonesia tidak memiliki hubungan diplomatik dengan Israel dan karena jalur langsung mudah dilacak. Barang dan lisensi bergerak melalui perusahaan perantara di Singapura, Malaysia, atau Luksemburg, yang sering memakai sekretaris perusahaan *nominee* sehingga pemilik sebenarnya sulit diketahui. Di Indonesia, perusahaan rekanan lokal memenangkan tender lalu menyerahkan sistem kepada lembaga negara (Amnesty International, 2024; Tim IndonesiaLeaks, 2023). Menurut narasumber IndonesiaLeaks, tidak lebih dari sepuluh perusahaan memegang lisensi NSO di Indonesia (Tim IndonesiaLeaks, 2023).

Barang dan lisensi bergerak melalui beberapa lapis perusahaan sebelum tiba di lembaga negara



Setiap lapis menyamarkan asal produk atau pemilik sebenarnya; dokumen tender tidak menyebut merek

Gambar 1. Rantai pengadaan alat penyadap dan *spyware* ke lembaga negara Indonesia
Sumber: disusun penulis berdasarkan Amnesty International (2024) dan Tim IndonesiaLeaks (2023).

Rantai berlapis seperti ini menyulitkan pengawasan dari dua arah. Negara pengekspor sulit memastikan siapa pengguna akhirnya, dan publik di negara pengimpor sulit mengetahui apa yang dibeli dengan uang pajak mereka. Israel, misalnya, menyatakan bahwa ekspor sistem pengawasan siber hanya diberikan kepada lembaga pemerintah untuk penegakan hukum dan antiterorisme, tetapi tidak memublikasikan informasi izinnya (Amnesty International, 2024).

6. Lapisan Ketiga: Jejak di Internet

Spyware membutuhkan infrastruktur: server untuk mengendalikan ponsel yang terinfeksi dan nama domain untuk tautan jebakan yang dikirim kepada sasaran. Infrastruktur ini memiliki sidik jari teknis yang dapat dikenali melalui pemindaian internet. Di lapisan inilah bukti tentang Indonesia paling beragam.

Jejak tertua menyangkut FinFisher. Citizen Lab menemukan server FinSpy di Indonesia pada 2013 dan pada 2015 mengaitkannya dengan Lembaga Sandi Negara, yang kemudian menjadi BSSN. Access Now pada 2018 juga menemukan aplikasi Android Indonesia tahun 2016 yang berisi FinSpy dan memakai domain *satgas.net*. Alamat IP yang sempat dituju domain itu berada dalam blok yang terkait dengan BNPT, tetapi buktinya belum cukup untuk memastikan BNPT sebagai pelanggan (Amnesty International, 2024).

Jejak NSO di lapisan ini tidak berupa Pegasus, melainkan Circles, perusahaan afiliasi NSO yang menjual sistem penyadap jaringan seluler. Sistem pengawasan Circles beroperasi di blok alamat IP yang terdaftar atas nama “RADIKA KARTA UTAMA” sejak September 2018 sampai setidaknya Desember 2020. Amnesty mengaitkan nama itu dengan PT Radika Karya Utama, pemenang tender alat sadap Polri, meskipun tidak menemukan perusahaan dengan nama persis seperti itu. Yang terpenting, Amnesty menyatakan tidak menemukan bukti bahwa Pegasus sendiri dipasang oleh Radika (Amnesty International, 2024). Temuan ini sejalan dengan laporan Citizen Lab tahun 2018 yang, melalui pemindaian internet pada 2016–2018, mendeteksi dugaan

infeksi Pegasus di 45 negara; Indonesia tidak termasuk di dalamnya (Marczak dkk., 2018). Ketiadaan Indonesia dalam daftar itu tidak membuktikan Pegasus tidak pernah dipakai, tetapi menunjukkan bahwa pada periode itu tidak ada aktivitas Pegasus terkait Indonesia yang terdeteksi oleh metode tersebut.

Jejak Candiru jauh lebih jelas. Pada Juli 2021, Citizen Lab dan Microsoft membongkar infrastruktur Candiru di berbagai negara dan mengidentifikasi sistem pelanggan yang diduga berada di Indonesia (Marczak dkk., 2021). Domain-domainnya, yang didaftarkan pada November 2020, meniru IndoProgress, TribunNews, Tirto, Media Indonesia, dan ANTARA. Sampai 2022 muncul domain yang meniru partai Gelora dengan pesan tentang pemindahan ibu kota dan domain yang meniru lembaga amal Islam (Amnesty International, 2024). Analisis Insikt Group (2025) menambahkan bahwa satu klaster infrastruktur Candiru yang sangat mungkin terkait pelanggan di Indonesia masih aktif sampai November 2024. Jika digabung dengan catatan pengiriman ke Polri pada 2020–2021, jejak Candiru mencapai tingkat B: dua lapisan independen menunjuk ke kesimpulan yang sama.

Jejak Predator, *spyware* buatan konsorsium Intellexa, tidak memiliki catatan pengiriman, tetapi infrastrukturnya terdeteksi. Server *backend* Predator di alamat IP Indonesia pertama kali terlihat pada Desember 2021 dan kemungkinan masih aktif pada Desember 2023. Domain jebakan paling awal yang terkait Indonesia, *ewestpapua.org* dan *nindonesia.news*, didaftarkan pada Maret 2022. Domain lain meniru situs “Suara Oposisi”, media Suara Papua, dan *geloraku.id*. Menurut Amnesty, domain-domain itu meniru situs partai oposisi serta media nasional dan lokal yang memiliki rekam jejak mendokumentasikan pelanggaran hak asasi manusia (Amnesty International, 2024). Selain itu, Wintego meninggalkan jejak berupa domain *tribunnews.org* yang meniru TribunNews pada Agustus 2018 dan domain yang menyamar sebagai pembaruan Samsung (Amnesty International, 2024).

Pemilihan domain itu memberi petunjuk tentang sasaran yang dibayangkan operatornya. Tautan yang tampak seperti berita Tirto, ANTARA, atau situs oposisi paling mungkin diklik oleh jurnalis, aktivis, politisi, dan pembaca yang mengikuti isu politik dan hak asasi manusia. Namun petunjuk bukan bukti. Amnesty sendiri menegaskan bahwa pihaknya tidak memiliki bukti bahwa teknologi tersebut telah dipakai terhadap anggota masyarakat sipil tertentu di Indonesia (Amnesty International, 2024). Klaim bahwa jurnalis, oposisi, dan kelompok kritis menjadi sasaran yang dibayangkan berada pada tingkat C.

7. Lapisan Keempat: Jejak di Ponsel Sasaran

Jejak dari sisi sasaran paling sedikit tersedia, tetapi satu peristiwa menonjol. Pada September 2022, Reuters melaporkan bahwa lebih dari selusin pejabat senior pemerintah dan militer Indonesia, termasuk diplomat dan penasihat, menjadi sasaran *spyware* pada 2021. Enam di antaranya mengaku menerima email dari Apple pada November 2021 yang menyatakan bahwa Apple meyakini mereka menjadi sasaran penyerang yang disponsori negara (Potkin dkk., 2022). Apple dan peneliti keamanan menyebut alat yang dipakai adalah ForcedEntry, eksploit tanpa klik yang pernah digunakan NSO. Seorang direktur BUMN pemasok senjata untuk TNI Angkatan Darat juga menerima peringatan yang sama (Malay Mail, 2022).

Peristiwa ini sering dikutip sebagai bukti Pegasus di Indonesia, padahal kesimpulannya lebih terbatas. Reuters tidak dapat memastikan siapa pembuat atau pengguna *spyware* itu, apakah serangannya berhasil, dan apa yang diperoleh penyerang. Perusahaan Israel lain, QuaDream,

diketahui memiliki alat yang hampir identik, dan NSO membantah keterlibatannya dengan menyebut hal itu mustahil secara kontrak dan teknologi (Potkin dkk., 2022). Karena sasarannya adalah pejabat negara sendiri, pelakunya bisa saja intelijen asing, bukan lembaga dalam negeri. Penargetan pejabat Indonesia dengan eksploit kelas NSO berada pada tingkat B, sedangkan identitas penyerangnya tetap tidak diketahui.

Klaim lain dari sisi sasaran lebih lemah. IndonesiaLeaks melaporkan dugaan pemantauan terhadap politisi menjelang Pemilu 2019 serta akademisi dan aktivis di Yogyakarta dan Bandung pada masa penolakan revisi UU KPK, dan menyebut dua belas pejabat tinggi pemerintah dan militer diduga menjadi sasaran (Tim IndonesiaLeaks, 2023). Hasil forensik dari ponsel para korban belum dipublikasikan, sehingga klaim ini berada pada tingkat C. Sampai kajian ini disusun, belum ada laporan forensik publik dari Citizen Lab, Amnesty, atau Access Now yang mengonfirmasi infeksi Pegasus pada ponsel warga Indonesia.

Konteks global tetap relevan. Apple mengirim gelombang peringatan *spyware* bayaran kepada pengguna di 110 negara pada Agustus 2026 dan menyarankan penerimanya segera mengaktifkan Lockdown Mode serta mencari bantuan ahli keamanan digital (Bisnis.com, 2026). Apple tidak menyebut negara mana saja yang terdampak, sehingga data ini tidak dapat dipakai untuk menyimpulkan apa pun tentang Indonesia secara khusus.

8. Lapisan Kelima: Jejak di Berkas Perkara

Skandal November 2026 membuka lapisan yang selama ini tertutup rapat. Untuk pertama kalinya, penyidik negara sendiri yang memaparkan bagaimana alat sadap dipakai di luar hukum.

Menurut Kabareskrim Komjen Asep Safrudin, para tersangka diduga memerintahkan penyadapan tanpa mengikuti prosedur dalam Peraturan Kapolri Nomor 5 Tahun 2010. Sejumlah nomor telepon dimasukkan ke server LIMS tanpa surat permohonan penyidik ataupun surat perintah (Tempo, 2026). Dalam rapat kerja dengan Komisi III DPR pada 12 November 2026, Kapolri Jenderal Suyudi Ario Seto memaparkan rantai perintahnya. Nomor sasaran dimasukkan ke LIMS tanpa diperiksa kaitannya dengan perkara pidana, lalu disadap memakai sistem PenLink X (PLX). Rekaman didengarkan, diekspor, dan dibuat transkripnya. Listyo Sigit diduga memberi perintah dan menentukan sasaran; Irjen Slamet Uliandi diduga menyetujui penyadapan dan meneruskan laporan harian serta laporan analisis kepada Listyo; Irjen Eko Hadi Santoso dan Irjen Ahrie Sonta, yang bergantian menjabat Plt. Kepala Bagian Monitoring, diduga meneruskan perintah kepada operator. Pada Oktober 2026, Ahrie Sonta diduga memerintahkan penghapusan rekaman dan log dari LIMS dan PLX, dan perintah inilah yang memicu pelaporan oleh staf pemantauan (CNN Indonesia, 2026).

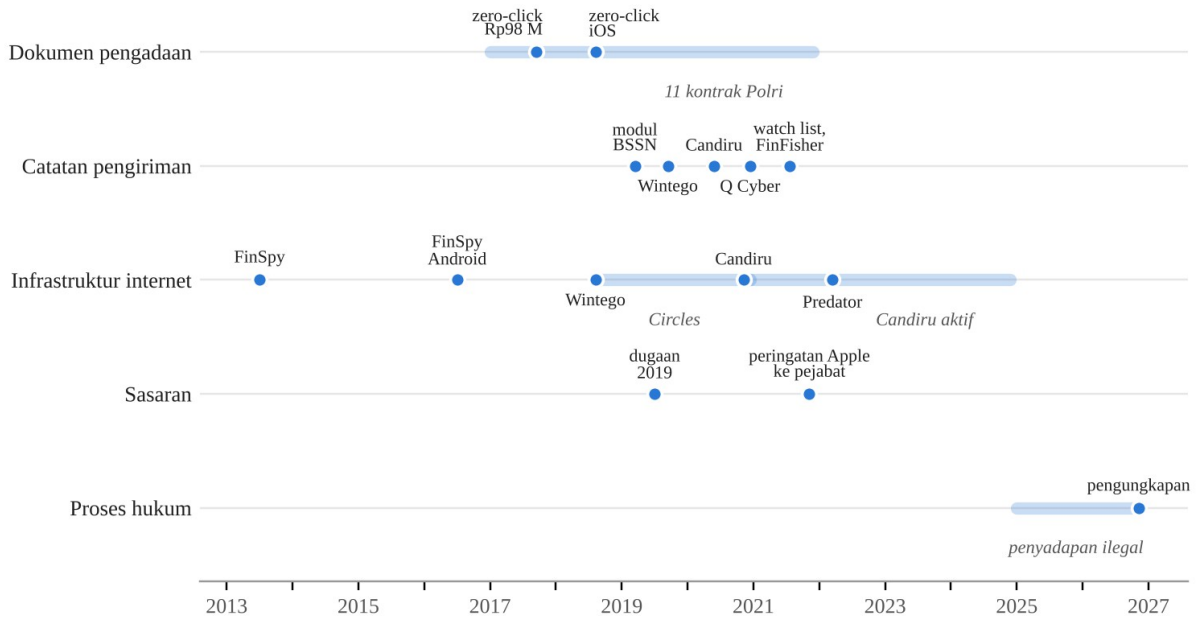
Kategori sasaran yang dipaparkan Kapolri sangat luas: Presiden dan lingkaran Istana, kementerian dan lembaga, anggota DPR dan partai politik, tokoh politik, gubernur dan kapolda, KPK, Kejaksaan Agung, internal Polri, organisasi masyarakat, aktivis, dan mahasiswa (CNN Indonesia, 2026). Polri belum mengumumkan jumlah nomor yang disadap (Tempo, 2026). Angka “6.000” dan “20.000 nomor” beredar luas, antara lain dari unggahan media sosial seorang mantan pejabat (Sindonews, 2026b), tetapi belum dikonfirmasi oleh penyidik dan karena itu berada pada tingkat D. Sampai 24 November 2026, tersangka bertambah menjadi enam orang dari kalangan Polri, termasuk Listyo Sigit, ditambah satu warga sipil berinisial NE, dan perkara berkembang ke dugaan makar (Viva, 2026; Detik, 2026).

Ada tiga pelajaran dari lapisan ini. Pertama, menurut keterangan penyidik, alat yang disalahgunakan bukan *spyware* rahasia, melainkan sistem sadap resmi yang dibeli secara sah untuk penegakan hukum. Kedua, penyalahgunaan diduga berlangsung sepanjang 2025–2026 tanpa terdeteksi oleh pengawasan internal, dan baru terbongkar karena staf di tingkat bawah menolak menghapus barang bukti. Ketiga, sasarannya tidak terbatas pada elite. Aktivis, organisasi masyarakat, dan mahasiswa ikut dipantau, sesuatu yang oleh Amnesty International Indonesia dinilai berpotensi menjadi pemolisian rahasia untuk menjinakkan oposisi, dengan korban yang bisa mencapai ratusan aktivis, jurnalis, politisi oposisi, dan pembela HAM (Amnesty International Indonesia, 2026).

Apakah Pegasus terlibat dalam skandal ini? Berdasarkan keterangan resmi, tidak ada bukti ke arah itu. Polri menyebut LIMS dan PLX, dan belum menyatakan adanya Pegasus (Medcom, 2026). Sebagian pakar menduga ada alat tanpa klik karena LIMS tidak dapat membaca isi aplikasi terenkripsi (Suara, 2026), tetapi dugaan itu belum didukung data. Seorang penulis telaah di Antara juga mencatat bahwa Polri tidak pernah menyatakan membeli Pegasus, meskipun kecurigaan itu tidak dapat diabaikan begitu saja (Wahyu S., 2026). Klaim bahwa skandal 2026 memakai Pegasus berada pada tingkat D.

9. Menimbang Seluruh Jejak

Gambar 2 menyusun seluruh jejak yang dibahas di atas menurut waktu dan lapisannya. Tampak bahwa jejak tidak muncul secara sporadis. Antara 2017 dan 2022, empat lapisan pertama aktif hampir bersamaan: tender dibuka, barang dikirim, server dinyalakan, domain jebakan didaftarkan, dan pejabat menerima peringatan. Lapisan kelima baru terbuka pada 2026. Pola ini mengisyaratkan pembangunan kemampuan pengawasan yang terencana dan berkelanjutan, bukan pembelian sesekali.



Gambar 2. Jejak alat penyadap di Indonesia menurut lapisan bukti, 2013–2026

Sumber: disusun penulis berdasarkan Amnesty International (2024), Tim IndonesiaLeaks (2023), Marczak dkk. (2018, 2021), Insikt Group (2025), Potkin dkk. (2022), dan CNN Indonesia (2026).

Tabel 2 merangkum penilaian atas klaim-klaim utama dengan skala dalam Tabel 1.

Tabel 2. Penilaian klaim utama tentang alat penyadap di Indonesia

Klaim	Tingkat	Dasar penilaian
Polri membeli sistem penyadapan tanpa klik sejak 2017 dengan anggaran ratusan miliar rupiah	A	Dokumen pengadaan elektronik; diverifikasi ICW
Sistem sadap resmi Polri (LIMS dan PLX) disalahgunakan untuk memantau Presiden, oposisi, aktivis, dan mahasiswa pada 2025–2026	A†	Keterangan resmi Kapolri dan Bareskrim; belum diuji di pengadilan
Sistem Candiru dipasok ke Polri dan infrastrukturnya aktif di Indonesia	B	Catatan pengiriman 2020–2021 dan infrastruktur 2020–2024 saling menguatkan
Sistem Wintego dipasok ke Polri	B	Catatan pengiriman 2019 dan infrastruktur 2018
Perangkat Q Cyber/NSO masuk ke Indonesia dan sistem Circles beroperasi	B	Manifes 2020 dan jejak IP 2018–2020
FinSpy beroperasi di Indonesia dan diatribusikan kepada Lembaga Sandi Negara (kini BSSN)	B	Pemindaian Citizen Lab 2013 dan 2015; sampel aplikasi Access Now 2018
Pejabat Indonesia diserang dengan eksploit kelas NSO pada 2021	B	Peringatan Apple kepada beberapa pejabat; identifikasi eksploit oleh peneliti; pelaku tidak diketahui
Infrastruktur Predator aktif di Indonesia	C	Pemindaian server dan domain; tidak ada catatan pengiriman; pemakai tidak diketahui
Media berita dan situs oposisi dijadikan umpan untuk menyasar pembacanya	C	Pola domain jebakan; belum ada korban terverifikasi
Polri memakai Pegasus secara spesifik	C	Narasumber anonim; dibantah Polri; tidak dikonfirmasi Amnesty
Skandal penyadapan 2026 memakai Pegasus	D	Spekulasi; tidak didukung keterangan resmi

Sumber: analisis penulis. †Tingkat A untuk adanya keterangan resmi penyidik; kebenaran materiilnya masih menunggu putusan pengadilan.

Dari penilaian ini dapat ditarik satu kesimpulan yang lebih tajam daripada perdebatan publik selama ini. Pertanyaan “apakah Indonesia memakai Pegasus” ternyata pertanyaan yang kurang tepat. Bukti untuk Pegasus secara spesifik justru yang paling lemah, sedangkan bukti untuk *spyware* lain yang sama invasifnya, terutama Candiru, jauh lebih kuat. Seperti dicatat pada bagian 2.1, *spyware* dengan kemampuan sedalam itu oleh Amnesty dinilai tidak mungkin digunakan secara sesuai dengan hak asasi manusia. Dengan demikian, persoalannya bukan merek tertentu, melainkan keberadaan kemampuan membobol ponsel di tangan lembaga yang tidak diawasi.

Penilaian ini juga perlu dibaca bersama keterbatasan bukti yang bersifat struktural. *Spyware* dirancang untuk tidak terdeteksi, transaksi dilakukan melalui perantara, dokumen pengadaan tidak dibuka, dan korban jarang memeriksakan ponselnya. Seorang pengamat siber yang dikutip Tempo bahkan menyatakan bahwa alat yang mudah terdeteksi berarti alat yang tidak bagus (Tempo, 2023). Karena itu, ketiadaan bukti forensik tidak sama dengan bukti bahwa *spyware* tidak dipakai.

10. Apakah Penggunaannya Sesuai Aturan Produsen?

10.1 Aturan yang dibuat produsen dan negara pengekspor

Spyware komersial tidak dijual tanpa syarat, setidaknya di atas kertas. Para produsen dan negara pengekspor menetapkan aturan tentang siapa yang boleh membeli dan untuk apa alat itu boleh dipakai. Pertanyaan yang jarang diajukan dalam perdebatan di Indonesia adalah apakah aturan-aturan itu dipatuhi.

NSO Group menyatakan bahwa teknologinya dirancang semata-mata untuk mencegah atau menyelidiki kejahatan serius dan terorisme, dan bahwa pelanggannya, yang seluruhnya lembaga pemerintah, wajib menyetujui syarat itu sebagai kondisi penggunaan (NSO Group, t.t.). Dalam laporan transparansi pertamanya, NSO menyebut setiap kontrak memuat klausul kepatuhan pada hak asasi manusia dan komitmen pelanggan untuk memakai sistemnya hanya bagi pencegahan dan penyelidikan kejahatan serius dan terorisme yang sah. Laporan yang sama mengakui bahwa pemantauan atas aktivitas pelanggan tetap menjadi tantangan besar karena NSO tidak memiliki pandangan langsung atas penggunaannya (Deccan Herald, 2021). NSO juga menyatakan berhak menangguhkan atau memutus pelanggan yang tidak mematuhi hukum dan peraturan domestik, dan menyatakan pernah melakukannya (NSO Group, 2020). Menurut laporan transparansinya, NSO menangguhkan atau memutus enam pelanggan pemerintah pada 2022–2023 dan memutus sistem lima pelanggan sejak 2016 setelah penyelidikan penyalahgunaan (TechCrunch, 2026). Candiru, menurut Citizen Lab, menjual *spyware* secara eksklusif kepada pemerintah (Marczak dkk., 2021).

Negara pengekspor menambahkan lapisan aturan sendiri. Israel hanya menyetujui ekspor sistem siber kepada lembaga pemerintah untuk penyelidikan dan pencegahan terorisme dan kejahatan (Israel National News, 2021). Pada 6 Desember 2021, Badan Pengendalian Ekspor Pertahanan Israel (DECA) memperketat deklarasi pengguna akhir yang wajib ditandatangani negara pembeli. “Kejahatan serius” didefinisikan sebagai tindak pidana dengan ancaman penjara enam tahun atau lebih menurut hukum negara pembeli, dan menyatakan pendapat atau kritik, termasuk tentang negara dan lembaganya, ditegaskan tidak dengan sendirinya merupakan tindakan teroris (Janes, 2021). Pelanggar komitmen itu akan langsung kehilangan akses atas sistem yang dibelinya (Jerusalem Post, 2021). Beberapa pekan sebelumnya, Israel memangkas daftar negara yang boleh membeli produk siber ofensif dari 102 menjadi 37 negara, sebagian besar negara Eropa Barat dan negara berbahasa Inggris; Indonesia tidak termasuk di dalamnya (Calcalist, 2021).

Amerika Serikat mengambil langkah lebih keras terhadap vendornya. NSO Group dan Candiru dimasukkan ke dalam *Entity List* Departemen Perdagangan AS pada November 2021. Entitas Intellexa dan Cytrox menyusul pada Juli 2023, dan Departemen Keuangan AS menjatuhkan sanksi kepada pendiri dan sejumlah entitas konsorsium Intellexa pada Maret 2024 (The Record, 2024b).

10.2 Menguji praktik di Indonesia

Dengan aturan-aturan itu sebagai ukuran, Tabel 3 membandingkan syarat yang ditetapkan produsen dan negara pengekspor dengan praktik yang terdokumentasi di Indonesia.

Tabel 3. Aturan produsen dan negara pengekspor dibandingkan dengan praktik di Indonesia

Aturan	Praktik yang terdokumentasi di Indonesia	Penilaian
Pembeli harus lembaga pemerintah	Pengguna akhirnya lembaga negara (Polri, BSSN), tetapi barang diterima dan tender dimenangkan perusahaan swasta dan broker di negara ketiga	Patuh secara formal, tetapi rantai perantara membuat produsen sulit memastikan pengguna akhir
Hanya untuk kejahatan serius dan terorisme	Domain jebakan meniru media dan partai oposisi; dugaan penyasaran akademisi dan aktivis pada 2019; menurut penyidik, sistem sadap resmi dipakai terhadap Presiden, KPK, aktivis, dan mahasiswa tanpa kaitan perkara pada 2025–2026	Indikasi penyimpangan untuk *spyware*; untuk sistem sadap resmi, penyimpangan diungkap penyidik
Kritik dan pendapat bukan terorisme (DECA, sejak Desember 2021)	Sasaran 2025–2026 mencakup organisasi masyarakat, aktivis, dan mahasiswa	Bertentangan, bila alat buatan Israel ikut dipakai; belum terbukti alat mana yang dipakai
Wajib patuh pada hukum domestik	Indonesia belum memiliki undang-undang penyadapan, dan tidak ada undang-undang yang mengatur pembobolan perangkat oleh aparat	Hampir tidak mungkin dipenuhi; tidak ada dasar hukum domestik untuk penggunaan *spyware*
Negara pembeli harus masuk daftar yang disetujui (Israel, sejak November 2021)	Indonesia tidak termasuk; kiriman Candiru terdokumentasi sampai Januari 2021 dan infrastrukturnya masih aktif sampai November 2024	Pasokan awal mendahului pengetatan; status dukungan teknis sesudahnya tidak diketahui
Produsen berhak memutus pelanggan yang menyalahgunakan	Tidak ada informasi publik bahwa produsen pernah menyelidiki atau memutus pelanggan di Indonesia	Mekanisme tidak terlihat bekerja

Sumber: analisis penulis berdasarkan NSO Group (t.t., 2020), Janes (2021), Calcalist (2021), Amnesty International (2024), Insikt Group (2025), dan CNN Indonesia (2026).

Tabel itu menunjukkan bahwa aturan yang paling mudah dipenuhi, yaitu syarat pembeli pemerintah, memang dipenuhi secara formal. Tetapi syarat-syarat yang menyangkut isi penggunaan memperlihatkan jarak yang lebar. Syarat “hanya untuk kejahatan serius dan terorisme” sulit dipercaya dipatuhi ketika domain jebakan dirancang meniru media berita dan partai oposisi, karena umpan semacam itu lebih cocok untuk menjangkau jurnalis, politisi, dan aktivis daripada pelaku kejahatan serius. Syarat kepatuhan pada hukum domestik bahkan hampir tidak mungkin dipenuhi, karena tidak ada undang-undang yang memberi dasar bagi pembobolan perangkat oleh aparat. Dengan kata lain, penggunaan *spyware* pembobol ponsel oleh lembaga negara Indonesia sulit dianggap memenuhi syarat yang ditetapkan produsennya sendiri.

Skandal 2026 memberi gambaran paling jelas tentang penyimpangan dari tujuan yang sah. Sistem yang disalahgunakan memang sistem sadap resmi, bukan *spyware* Israel. Namun pola penyimpangannya adalah pola yang dikhawatirkan oleh semua aturan produsen dan eksportir: sasaran ditentukan lewat pesan WhatsApp tanpa perkara pidana, mencakup aktivis dan mahasiswa, dan hasilnya mengalir kepada satu orang di puncak hierarki (CNN Indonesia, 2026). Jika sistem yang terikat prosedur internal dan meninggalkan jejak di operator dapat disalahgunakan seperti itu, tidak ada alasan untuk berasumsi bahwa *spyware* yang tidak meninggalkan jejak diperlakukan lebih hati-hati.

Ada pula persoalan waktu. Kiriman perangkat yang dinilai Amnesty sebagai sistem Candiru terjadi antara Mei 2020 dan Januari 2021, dan lisensi "watch list" Wintego dikirim pada Juli 2021, semuanya sebelum Israel memperketat daftar negara pembeli pada November 2021 (Amnesty International, 2024; Calcalist, 2021). Namun infrastruktur Candiru yang terkait pelanggan di Indonesia dilaporkan masih aktif sampai November 2024 (Insikt Group, 2025). *Spyware* semacam ini biasanya memerlukan pembaruan eksploit dan dukungan teknis berkala dari vendornya. Data yang tersedia tidak memungkinkan kesimpulan tentang apakah dukungan semacam itu berlanjut setelah Indonesia keluar dari daftar ekspor Israel, tetapi pertanyaan itu layak diajukan kepada pemerintah Israel, vendor, dan lembaga pengguna di Indonesia.

Pernyataan NSO kepada Amnesty juga perlu dibaca dengan cermat. NSO menyatakan tidak menyediakan sistem geolokasi aktif atau sistem pembobol ponsel kepada Indonesia berdasarkan prosedur uji tuntasnya yang berlaku saat ini (Amnesty International, 2024). Frasa "yang berlaku saat ini" tidak menjawab pertanyaan tentang masa sebelum prosedur itu diterapkan, tidak menyangkut afiliasinya, Circles, yang sistemnya tercatat beroperasi di Indonesia pada 2018–2020, dan tidak menjelaskan kiriman perangkat dari Q Cyber pada Desember 2020.

Akhirnya, mekanisme pengaman yang dijanjikan produsen tidak terlihat bekerja di Indonesia. NSO sendiri mengakui tidak memiliki pandangan langsung atas penggunaan sistemnya, sementara Candiru menolak membahas lisensinya dengan alasan hukum (Amnesty International, 2024). Tidak ada informasi publik bahwa vendor mana pun pernah menyelidiki atau memutus pelanggan di Indonesia. Aturan produsen, dengan demikian, berfungsi lebih sebagai perlindungan reputasi bagi penjual daripada perlindungan bagi orang yang disadap. Pengendalian yang sungguh-sungguh hanya mungkin datang dari hukum dan lembaga pengawas di negara pengguna, dan di situlah Indonesia paling lemah.

11. Mengapa Hukum Tidak Mampu Mengendalikan

11.1 Mandat yang tidak dilaksanakan

Konstitusi menjamin hak atas rasa aman dan perlindungan diri pribadi dalam Pasal 28G ayat (1) serta hak berkomunikasi dalam Pasal 28F UUD 1945. Jaminan itu diperkuat Pasal 17 Kovenan Internasional tentang Hak-Hak Sipil dan Politik yang telah diratifikasi (lihat bagian 2.2). Penyadapan adalah pembatasan hak, sehingga menurut Pasal 28J ayat (2) UUD 1945 hanya dapat dilakukan berdasarkan undang-undang.

Mahkamah Konstitusi sudah menegaskan hal itu. Dalam Putusan Nomor 5/PUU-VIII/2010 yang dibacakan pada 24 Februari 2011, Mahkamah membatalkan Pasal 31 ayat (4) UU ITE yang menyerahkan tata cara penyadapan kepada peraturan pemerintah, dan menegaskan bahwa penyadapan harus diatur dengan undang-undang (Putusan MK Nomor 5/PUU-VIII/2010). Lima belas tahun kemudian, undang-undang itu belum ada. KUHAP baru, yaitu UU Nomor 20 Tahun 2025 yang berlaku sejak 2 Januari 2026, hanya mendefinisikan penyadapan dan menyerahkan pengaturannya kepada undang-undang khusus. Syarat, jangka waktu, mekanisme izin pengadilan, penyimpanan, dan pemusnahan hasil sadapan belum diatur (Hukumonline, 2026).

11.2 Aturan yang terpecah-pecah

Dalam kekosongan itu, kewenangan menyadap tersebar di berbagai undang-undang dengan syarat yang berbeda-beda. Undang-Undang Telekomunikasi pada prinsipnya melarang penyadapan dalam Pasal 40, lalu memberi pengecualian dalam Pasal 42 ayat (2): untuk keperluan peradilan pidana, operator dapat merekam dan memberikan informasi atas permintaan tertulis Jaksa Agung dan/atau Kapolri untuk tindak pidana tertentu, atau atas permintaan penyidik sesuai undang-undang yang berlaku (Hukumonline, 2009). Undang-undang sektoral kemudian mengatur kewenangan masing-masing lembaga, seperti dirangkum dalam Tabel 4.

Tabel 4. Kewenangan penyadapan menurut undang-undang sektoral

Lembaga	Dasar hukum	Otorisasi	Jangka waktu
KPK	UU 19/2019 Pasal 12 dan 12C jo. Putusan MK 70/PUU-XVII/2019	Tanpa izin; dipertanggungjawabkan kepada pimpinan dan diberitahukan kepada Dewan Pengawas paling lambat 14 hari kerja setelah selesai	Tidak lagi diatur sejak Pasal 12B dibatalkan
Penyidik narkotika	UU 35/2009 Pasal 77–78	Izin tertulis ketua pengadilan negeri; dalam keadaan mendesak, izin diminta paling lama 1×24 jam sesudahnya	3 bulan, dapat diperpanjang satu kali
Penyidik terorisme	UU 15/2003 jo. UU 5/2018 Pasal 31–31A	Izin tertulis ketua pengadilan negeri; dalam keadaan mendesak, pemberitahuan paling lama 3 hari sesudahnya	1 tahun, dapat diperpanjang satu kali
Penyidik perdagangan orang	UU 21/2007 Pasal 31	Izin tertulis ketua pengadilan	Paling lama 1 tahun
BIN	UU 17/2011 Pasal 31–32	Perintah Kepala BIN; penetapan ketua pengadilan negeri bila sasaran sudah memiliki bukti permulaan yang cukup	6 bulan, dapat diperpanjang sesuai kebutuhan
Polri (umum)	UU 36/1999 Pasal 42 ayat (2); Perkap 5/2010	Permintaan tertulis Kapolri atau penyidik; prosedur internal	Diatur internal
Kejaksaan	UU 11/2021 Pasal 30C huruf i	Digantungkan pada undang-undang khusus tentang penyadapan yang belum ada	Belum diatur

Sumber: diolah dari undang-undang terkait, Putusan MK Nomor 70/PUU-XVII/2019, Detik (2021), Hikmawati (2022), Hukumonline (2009, 2017), dan Saidin (2026).

Tabel itu memperlihatkan ketidakseragaman dalam dua hal. Dari segi otorisasi, ada lembaga yang wajib meminta izin pengadilan, ada yang cukup memberi tahu pengawas internal, dan ada yang hanya mengandalkan prosedur internal. Dari segi waktu, jangka penyadapan beragam, dari tiga bulan sampai satu tahun dengan kemungkinan perpanjangan, bahkan tanpa batas yang jelas (Saidin, 2026). Bagi KPK, batas enam bulan ikut gugur ketika Mahkamah membatalkan Pasal 12B seluruhnya (Putusan MK Nomor 70/PUU-XVII/2019). Hikmawati (2022) mencatat bahwa ketidakseragaman ini menimbulkan ketidakpastian hukum, dan bahwa putusan MK tentang KPK pun belum memenuhi seruan MK sebelumnya agar ada undang-undang khusus yang menunjuk otoritas pemberi izin. Polri, lembaga yang paling banyak membeli alat sadap,

justru bekerja dengan dasar yang paling lemah, yaitu Peraturan Kapolri Nomor 5 Tahun 2010, yang menurut YLBHI tidak lagi sinkron dengan perkembangan hukum dan mandat putusan MK (Kontan, t.t.). Undang-Undang Intelijen Negara menempatkan penyadapan di bawah perintah Kepala BIN dan hanya mensyaratkan penetapan pengadilan bila sasaran sudah memiliki bukti permulaan yang cukup (Detik, 2021), dan para ahli sejak awal menilai mekanisme serta otorisasinya tidak diatur secara ketat (Hukumonline, 2012).

Bila diukur dengan 13 Prinsip Kebutuhan dan Proporsionalitas, hasilnya jelas. Prinsip **legalitas** tidak terpenuhi bagi Polri karena tata cara penyadapannya hanya diatur dalam peraturan internal, bukan dalam undang-undang sebagaimana diperintahkan Mahkamah Konstitusi. Prinsip **otoritas peradilan** hanya terpenuhi sebagian, untuk tindak pidana tertentu. Prinsip **pemberitahuan kepada pengguna** tidak dikenal di undang-undang mana pun: tidak ada kewajiban memberi tahu orang yang disadap, bahkan setelah perkara selesai. Prinsip **transparansi** dan **pengawasan publik** juga tidak terpenuhi, karena tidak ada laporan berkala tentang jumlah penyadapan, dan dokumen pengadaannya tertutup. Akibatnya, prinsip **tujuan sah**, **kebutuhan**, dan **proporsionalitas** tidak dapat diuji secara bermakna: tanpa hakim atau lembaga independen yang memeriksa alasan setiap penyadapan sebelum dilakukan, tidak ada yang menimbang apakah penyadapan itu perlu dan sebanding dengan kerugian bagi hak orang yang disadap.

Skandal 2026 menunjukkan akibatnya. Prosedur internal Polri mensyaratkan surat permohonan penyidik, tetapi syarat itu dapat dilangkahi dengan perintah lisan atau pesan WhatsApp dari pimpinan tertinggi. Tidak ada hakim yang memberi izin sebelum penyadapan, tidak ada pihak luar yang memeriksa daftar nomor, dan tidak ada audit berkala atas log sistem. Pengaman yang akhirnya bekerja tampaknya hanyalah hati nurani beberapa staf yang menolak menghapus jejak.

11.3 Spyware: wilayah tanpa aturan sama sekali

Jika penyadapan melalui operator saja tidak diatur dengan baik, *spyware* berada di wilayah yang lebih gelap lagi. Indonesia tidak memiliki undang-undang yang mengatur penggunaan *spyware* dan teknologi pengawasan secara sah (Al Jazeera, 2024). Perbedaannya penting secara teknis maupun hukum. LIMS bekerja melalui jaringan operator telekomunikasi dan setidaknya meninggalkan jejak di sisi operator. *Spyware* seperti Pegasus atau Candiru bekerja dengan membobol ponsel itu sendiri, sehingga tidak melewati operator sama sekali dan mampu membaca isi aplikasi terenkripsi, foto, dokumen, serta menyalakan mikrofon dan kamera (Medcom, 2026). Pembobolan seperti ini lebih tepat disebut peretasan daripada penyadapan. UU ITE mengancam pidana akses ilegal ke sistem elektronik (Pasal 30) dan intersepsi ilegal (Pasal 31). Pasal 31 memang mengecualikan intersepsi oleh penegak hukum, tetapi hanya bila dilakukan berdasarkan undang-undang. Karena tidak ada undang-undang yang mengatur pembobolan perangkat oleh aparat, pengecualian itu sulit diterapkan. Ketika lembaga negara melakukannya, yang terjadi adalah peretasan oleh negara tanpa payung hukum.

11.4 Pengawasan pengadaan yang tumpul

Celah terakhir menyangkut pengadaan. Dokumen tender alat sadap diperlakukan sebagai rahasia, sehingga publik dan bahkan DPR tidak mengetahui apa yang dibeli (Bisnis.com, 2023a). Permintaan ICW pada 2023 tidak dijawab memadai, dan atas laporan Amnesty pada 2024, Polri menerima surat tetapi menolak menjawab pertanyaan, sementara BSSN tidak merespons (Amnesty International, 2024). DPR baru menanyakan keberadaan fisik alat sadap

Polri setelah skandal 2026 mencuat (Katadata, 2026). Pengawasan yang hanya bergerak setelah skandal lebih menyerupai pemadaman kebakaran daripada pengawasan.

12. Belajar dari Negara Lain

Indonesia bukan satu-satunya negara yang menghadapi skandal *spyware*, dan pengalaman negara lain menunjukkan jalan yang dapat ditempuh setelah skandal terbongkar.

Polandia memberikan contoh paling relevan. Pemerintahan baru yang terbentuk pada akhir 2023 membuka penggunaan Pegasus oleh pemerintahan sebelumnya. Jaksa Agung Adam Bodnar melaporkan kepada parlemen bahwa Pegasus dipakai terhadap 578 orang pada 2017–2022 oleh tiga lembaga, yaitu Biro Antikorupsi Pusat, Dinas Kontraintelijen Militer, dan Badan Keamanan Dalam Negeri (Associated Press, 2024). Parlemen membentuk komisi penyelidikan khusus, dan jaksa memanggil para korban untuk diperiksa. Peneliti Citizen Lab menyebut keterbukaan data korban oleh pemerintah Polandia sebagai yang pertama di Uni Eropa (The Record, 2024a). Proses itu tidak mulus, karena Tribunal Konstitusi Polandia, yang independensinya dipersoalkan, menyatakan komisi tersebut inkonstitusional, tetapi komisi tetap bekerja (Notes from Poland, 2024).

Di tingkat Uni Eropa, Parlemen Eropa membentuk Komite Penyelidikan Penggunaan Pegasus dan *Spyware* Sejenis (PEGA). Komite ini menyimpulkan bahwa *spyware* telah dipakai untuk melanggar hak-hak dasar dan membahayakan demokrasi di beberapa negara anggota, dengan Polandia dan Hungaria sebagai kasus paling mencolok (European Parliament, 2023). Pada 15 Juni 2023, Parlemen Eropa mengadopsi rekomendasi reformasi dan secara khusus meminta Polandia, Hungaria, Yunani, Spanyol, dan Siprus menindaklanjuti pelanggaran yang terjadi (Eucrim, 2023). Di Yunani, telah dikonfirmasi bahwa seorang anggota Parlemen Eropa dan seorang jurnalis disadap oleh dinas intelijen dan menjadi sasaran *spyware* Predator (Parliamentary Assembly of the Council of Europe, 2023).

Di tingkat global, inisiatif multilateral mulai terbentuk. Proses Pall Mall, yang diluncurkan Inggris dan Prancis pada Februari 2024, menghasilkan Kode Praktik bagi Negara pada April 2025. Kode ini bersifat sukarela dan tidak mengikat, tetapi menetapkan praktik baik bagi negara dalam mengembangkan, memfasilitasi, membeli, mengalihkan, dan menggunakan kemampuan intrusi siber komersial (UK Government, 2025). Kode itu bertumpu pada empat pilar: akuntabilitas, presisi, transparansi, dan pengawasan (CyberScoop, 2025). Penandatangan awalnya sebagian besar negara Eropa, ditambah Jepang dan Ghana, dan Indonesia tidak termasuk di antaranya (YesWeHack, 2025).

Tiga pelajaran dapat ditarik untuk Indonesia. Pertama, skandal dapat menjadi titik balik bila diikuti pengungkapan menyeluruh: jumlah korban, lembaga pengguna, dan dasar hukum setiap penyadapan, seperti yang dilakukan Polandia. Kedua, penyelidikan oleh parlemen hanya efektif bila lembaga pengawas tetap independen; Parlemen Eropa mencatat bahwa di Polandia dan Hungaria, pembongkaran mekanisme pengawasan independen justru menjadi akar penyalahgunaan (European Parliament, 2023). Ketiga, Indonesia dapat memanfaatkan kerangka internasional seperti Kode Praktik Pall Mall sebagai patokan untuk menyusun undang-undangnya sendiri, tanpa harus memulai dari nol.

13. Simpulan dan Rekomendasi

13.1 Simpulan

Penelusuran atas lima lapisan jejak serta pengujiannya terhadap standar hak asasi manusia dan syarat produsen menghasilkan empat simpulan, yang sekaligus menjawab empat pertanyaan kajian.

Pertama, Indonesia memiliki ekosistem alat penyadap yang besar, berlapis, dan tertutup. Polri membeli sistem penyadapan tanpa klik sejak 2017 dengan anggaran ratusan miliar rupiah, dan produk dari sedikitnya lima vendor *spyware* dan alat pengawasan, yakni Candiru, Wintego, Circles/Q Cyber, FinFisher, dan Predator, meninggalkan jejak di Indonesia antara 2013 dan 2024. Barang-barang itu masuk melalui jaringan perantara di Singapura, Malaysia, dan Luksemburg yang menyamarkan asal dan tujuannya.

Kedua, penggunaan Pegasus secara spesifik oleh lembaga negara Indonesia belum terbukti secara terbuka. Bukti untuk Pegasus justru yang paling lemah dibandingkan bukti untuk *spyware* lain yang sama invasifnya. Pusat perhatian publik pada satu merek telah mengaburkan persoalan yang lebih besar dan memudahkan penyangkalan.

Ketiga, skandal penyadapan 2025–2026, menurut keterangan resmi penyidik yang belum diuji di pengadilan, menunjukkan bahwa sistem sadap resmi dapat disalahgunakan secara luas untuk memantau Presiden, lembaga negara, oposisi, aktivis, organisasi masyarakat, dan mahasiswa tanpa terdeteksi oleh pengawasan internal. Jika sistem yang meninggalkan jejak di operator saja dapat disalahgunakan seluas ini, risiko dari *spyware* yang tidak meninggalkan jejak jauh lebih besar.

Keempat, akar persoalannya adalah kekosongan hukum dan pengawasan, sehingga baik standar hak asasi manusia maupun syarat produsen tidak dapat ditegakkan. Lima belas tahun setelah putusan MK, Indonesia belum memiliki undang-undang penyadapan, tidak memiliki aturan tentang *spyware*, dan tidak membuka dokumen pengadaan alat sadap. Domain jebakan yang meniru media berita dan situs oposisi menunjukkan bahwa jurnalis, oposisi, dan kelompok kritis adalah yang paling rentan dalam kekosongan ini. Syarat yang ditetapkan produsen dan negara pengekspor tidak mengisi kekosongan itu: syarat penggunaan untuk kejahatan serius tidak terlihat dipenuhi, syarat kepatuhan pada hukum domestik hampir mustahil dipenuhi, dan mekanisme pemutusan pelanggan tidak terlihat bekerja.

13.2 Rekomendasi

1. Pemerintah perlu memberlakukan moratorium pembelian dan penggunaan *spyware* pembobol ponsel oleh seluruh lembaga negara sampai ada undang-undang yang mengaturnya sesuai standar hak asasi manusia, sejalan dengan seruan Pelapor Khusus PBB (Kaye, 2019), Kantor Komisaris Tinggi HAM PBB (OHCHR, 2022), dan Amnesty International Indonesia (2026).
2. DPR dan Pemerintah perlu menyusun UU Penyadapan yang menyeragamkan kewenangan seluruh lembaga, mewajibkan izin pengadilan sebelum penyadapan, membatasi jangka waktu dan jenis tindak pidana, mengatur penyimpanan dan pemusnahan hasil sadapan, serta mewajibkan pemberitahuan kepada orang yang disadap setelah penyadapan selesai bila tidak lagi membahayakan penyidikan. Undang-undang itu

harus mengatur *spyware* secara terpisah dan jauh lebih ketat daripada penyadapan melalui operator, atau melarangnya sama sekali.

3. Pembahasan RUU Penyadapan yang dimulai kembali pada November 2026 (Sindonews, 2026a) perlu dilakukan secara terbuka dan melibatkan masyarakat sipil, agar suasana darurat setelah skandal tidak justru melahirkan undang-undang yang melegalkan kewenangan sadap yang luas.
4. BPK dan lembaga pengawas independen perlu mengaudit seluruh pengadaan alat sadap dan *spyware* oleh Polri, BSSN, BIN, dan lembaga lain sejak 2017, termasuk keberadaan fisik, status operasional, dan log penggunaannya. Hasil audit perlu dilaporkan kepada DPR dalam forum yang dapat dipertanggungjawabkan kepada publik.
5. Penyidikan skandal 2026 tidak boleh berhenti pada dimensi keamanan negara dan dugaan makar. Polri perlu mengungkap jumlah korban, kategori, dan dasar setiap penyadapan, seperti yang dilakukan Polandia. Korban dari kalangan aktivis, jurnalis, organisasi masyarakat, dan mahasiswa perlu diberi tahu, diberi akses atas data yang dikumpulkan tentang mereka, dan mendapat pemulihan. Pembentukan komite independen yang melibatkan masyarakat sipil, sebagaimana diusulkan Amnesty International Indonesia (2026), patut dipertimbangkan.
6. Pemerintah perlu meminta penjelasan resmi dari negara pengekspor dan vendor tentang izin ekspor, pengguna akhir, dan dukungan teknis atas sistem yang dipasok ke Indonesia, serta menyatakan keikutsertaan dalam Proses Pall Mall dan menjadikan Kode Praktiknya sebagai patokan penyusunan undang-undang.
7. Lembaga yang berwenang menyadap perlu menerbitkan laporan transparansi tahunan tentang jumlah permohonan, izin, dan penyadapan yang dilakukan, sejalan dengan prinsip transparansi dan pengawasan publik dalam 13 Prinsip Kebutuhan dan Proporsionalitas.
8. Masyarakat sipil, khususnya organisasi pembela HAM, jurnalis, pengacara, dan kelompok advokasi, perlu memperkuat kapasitas keamanan digital: pembaruan perangkat secara rutin, Lockdown Mode bagi yang berisiko tinggi, kewaspadaan terhadap tautan yang meniru media, serta pemeriksaan forensik melalui Access Now Digital Security Helpline atau Amnesty Security Lab bila ada kecurigaan. Dokumentasi kolektif atas dugaan serangan adalah bukti yang selama ini paling kurang dalam kasus Indonesia.

Penelusuran ini dimulai dengan pertanyaan tentang satu nama, tetapi berakhir pada persoalan yang lebih mendasar. Yang perlu dicari bukan lagi jejak Pegasus semata, melainkan jejak akuntabilitas: siapa yang membeli, siapa yang memakai, siapa yang mengawasi, dan siapa yang melindungi warga yang disadap. Selama pertanyaan-pertanyaan itu tidak dapat dijawab dari dokumen resmi, warga negara terpaksa mencari jawabannya sendiri dari manifes kargo, server di internet, dan keberanian segelintir staf yang menolak menghapus barang bukti.

Daftar Pustaka

Al Jazeera. (2024, 3 Mei). *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 Mei). *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* [Siaran pers]. 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 Oktober). *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 Juni). *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 Agustus). *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 Juli). *EP recommendation on lessons learned from misused spyware*. https://eucrim.eu/news/ep-recommendation-on-lessons-learned-from-misused-spyware/

European Parliament. (2023, 9 Mei). *Spyware: MEPs sound alarm on threat to democracy and demand reforms* [Siaran pers]. 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). *[Analisis ancaman siber tentang infrastruktur spyware Candiru]* (CTA-2025-0805). Recorded Future. https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf

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

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

Jerusalem Post. (2021, 7 Desember). *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. (t.t.). *YLBHI desak DPR segera bentuk UU Penyadapan*. https://nasional.kontan.co.id/news/ylbhi-desak-dpr-segera-bentuk-uu-penyadapan

Kumparan. (2023, 9 Oktober). *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. (t.t.). *NSO Group reply* [Tanggapan kepada Business & Human Rights Resource Centre]. https://www.business-humanrights.org/documents/5269/NSO_Group_reply.pdf

NSO Group. (2020, 2 Juni). *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 (dari 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 Juni). *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 Juni). *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.

Cara Mengutip (APA 7)

Dumupa, Y. (2026). *Mencari jejak alat penyadap di Indonesia* [Kajian ilmiah]. Yakobus Dumupa. https://yakobusdumupa.com/kajian/mencari-jejak-alat-penyadap-di-indonesia