

MILITERISASI TEKNOLOGI DI INDONESIA

DAN IMPLIKASINYA TERHADAP
HAK ASASI MANUSIA



MILITERISASI TEKNOLOGI DI INDONESIA

**Dan IMPLIKASINYA TERHADAP
HAK ASASI MANUSIA**

MILITERISASI TEKNOLOGI DI INDONESIA

Dan IMPLIKASINYA TERHADAP HAK ASASI MANUSIA

Penulis

Gina Sabrina
Annisa Azzahra
Kezia Khatwani

Editor

Ferinda

Ilustrasi & Layout

Amry Al Mursaat
Dodi Sanjaya

Penerbit

Lembaga Studi dan Advokasi Masyarakat (ELSAM) 2026

Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510



DAFTAR ISI

PENGANTAR	1
PEMBAHASAN	2
Kesenjangan Kemajuan Teknologi v. Pengaturannya	2
UU Intelijen dan Ketiadaan Pengawasan Yudisial	6
Lemahnya <i>Check and Balances</i> dalam Pengawasan Digital: <i>spyware</i> sebagai Zona Bebas Akuntabilitas	11
Dominasi Penunjukan Langsung dalam Pengadaan Sistem Pertahanan	21
Rantai Pasok yang Kabur, Biaya yang Tinggi, dan Tidak Transparan	22
Sekuritisasi dan Narasi Keamanan Nasional dalam Pengadaan Sistem Pertahanan	24
Lemahnya Mekanisme Pengawasan	25
Gagasan Perlindungan Hukum dan HAM dalam Lanskap Digital	26
PENUTUP	28
Kesimpulan	28
Rekomendasi	28
DAFTAR PUSTAKA	31

MILITERISASI TEKNOLOGI DI INDONESIA DAN IMPLIKASINYA TERHADAP HAK ASASI MANUSIA

PENGANTAR

Lanskap keamanan global tengah mengalami transformasi seiring meningkatnya peran teknologi digital dalam pertahanan dan keamanan. Kekuatan militer suatu negara kini tidak lagi diukur hanya dari kekuatan persenjataan konvensional, tetapi juga dari kemampuan negara tersebut memanfaatkan teknologi digital untuk mendukung operasi di ruang siber. Perubahan tersebut mendorong semakin luasnya penggunaan berbagai teknologi digital, termasuk teknologi surveilans (*surveillance technology*), sebagai bagian dari strategi keamanan. Dalam perkembangannya, teknologi ini tidak hanya dimanfaatkan untuk menghadapi ancaman keamanan nasional, tetapi juga digunakan untuk mengawasi aktivitas warga negara di luar tujuan keamanan yang sah.

Perubahan ini ditandai oleh semakin luasnya pemanfaatan teknologi *dual-use* (*dual-use technology*), yaitu teknologi yang dapat dimanfaatkan untuk kepentingan sipil maupun militer. Beberapa contoh dari teknologi fungsi ganda ini adalah drone, satelit, *cloud computing*, dan kecerdasan buatan (*artificial intelligence/AI*). Teknologi tersebut dimanfaatkan telah digunakan untuk mendukung aktivitas sipil, layanan publik, dan kepentingan komersial. Seiring perkembangannya, teknologi yang sama juga digunakan untuk kepentingan pertahanan, surveilans, dan operasi militer.¹ Karakter *dual-use* tersebut turut mendorong militerisasi teknologi, yakni semakin dominannya logika pertahanan dan keamanan dalam pengembangan dan penggunaan teknologi digital.

Salah satu manifestasi dari militerisasi teknologi adalah penggunaan *spyware* sebagai instrumen surveilans oleh negara. Laporan berbagai organisasi seperti Citizen Lab, dan Amnesty International mengungkapkan bahwa *spyware* telah digunakan untuk memata-matai jurnalis, aktivis demokrasi, dan pembela hak asasi manusia di berbagai negara. Di Indonesia, risiko penyalahgunaan *spyware* semakin besar ketika perluasan kewenangan aktor keamanan di ruang digital tidak diimbangi dengan mekanisme pengawasan yang efektif. Kondisi tersebut membuka ruang bagi penggunaan teknologi surveilans di luar tujuan keamanan yang sah serta berpotensi mengancam hak atas privasi, kebebasan berekspresi, dan kualitas demokrasi.

Militerisasi teknologi telah meningkatkan risiko pelanggaran hak asasi manusia, khususnya terhadap hak atas privasi, kebebasan berekspresi, dan kebebasan berpendapat. Tanpa

¹ Privacy International, "Investigating Dual-Use Technology and the Darker Side of Innovation," 10 November 2025, <https://privacyinternational.org/long-read/5705/investigating-dual-use-technology-and-darker-side-innovation>.

kerangka hukum yang jelas serta mekanisme pengawasan yang akuntabel, penggunaan teknologi surveilans berpotensi berubah menjadi instrumen represi digital yang tidak tersentuh hukum. Oleh karena itu, kertas kebijakan ini disusun untuk mendorong pengaturan yang komprehensif mengenai pengadaan dan penggunaan teknologi surveilans, khususnya *spyware*, agar tetap tunduk pada prinsip negara hukum, demokrasi, dan hak asasi manusia. Dengan demikian, penguatan keamanan nasional dapat berjalan seiring dengan perlindungan hak-hak konstitusional warga negara.

PEMBAHASAN

Kesenjangan Kemajuan Teknologi v. Pengaturannya

Indonesia turut mengalami transformasi fundamental dalam pendekatan keamanan nasional. Pergeseran tersebut mengikuti perubahan lanskap global dan peningkatan penggunaan teknologi surveilans komersial, yang mendorong pertahanan keamanan nasional konvensional menjadi *surveillance-based security*. Pendekatan keamanan kini tidak lagi bergantung pada kekuatan militer secara fisik, namun juga pada kemampuan memantau, mengumpulkan dan menganalisis data menggunakan teknologi. Hal ini sedang masif terjadi khususnya di perang Ukraina dan Gaza, serta ekspansi jalur sutra digital China. Persoalan timbul ketika percepatan perkembangan teknologi surveilans menciptakan ekosistem yang semakin menyulitkan untuk membedakan teknologi militer dan sipil, khususnya tanpa *safeguard* yang jelas untuk memisahkan keduanya. Pergeseran arah pertahanan saat ini secara global juga mengandung paradoks berbahaya. Di satu sisi ada upaya memperkuat keamanan, tapi pada saat bersamaan upaya tersebut menciptakan ancaman baru terhadap hak asasi manusia dan demokrasi.

Secara kontekstual di Indonesia terjadi kenaikan anggaran sebesar 22% di bawah pemerintahan Prabowo, kenaikan ini termasuk juga untuk menopang tidak hanya kekuatan militer konvensional melainkan juga militer yang berbasis teknologi surveilans. Dengan catatan penting bahwa di tahun 2025 DPR RI telah mengesahkan revisi UU TNI. Isi dari UU TNI yang telah direvisi ini memperluas kewenangan militer untuk masuk ke ranah dan ruang-ruang sipil, sehingga pemisahan antara militer dan sipil menjadi semakin kabur.²

Pada 2025, pemerintah semakin agresif dalam mendorong pengembangan kerja sama industri teknologi pertahanan. Salah satu inisiatif penting adalah adanya penyelenggaraan Defence Technology Forum 2025 di Jakarta, yang digagas oleh Badan Teknologi Pertahanan (Batekhan) Kementerian Pertahanan RI bersama perusahaan industri pertahanan asal Prancis, Krauss-Maffei Wegmann dan Nexter Defense Systems

² BBC News Indonesia, "Demonstrasi mahasiswa menentang UU TNI berlangsung maraton dan menyebar ke banyak kota, apa maknanya?," *BBC News Indonesia*, 31 Maret 2025, <https://www.bbc.com/indonesia/articles/c0jgj0e4284o> (diakses pada 20 Januari 2026).

(KNDS).³ Kolaborasi dengan KNDS tidak hanya diarahkan untuk agenda terkait pengadaan alat utama sistem persenjataan (alutsista), tetapi juga memperkuat agenda transfer teknologi, peningkatan kapasitas sumber daya manusia, serta pengembangan basis manufaktur pertahanan dalam negeri.⁴

Selain itu, pemerintah juga memperluas diplomasi pertahanan dengan sejumlah negara. di 2025 Menteri Pertahanan melakukan kunjungan ke Tiongkok untuk bertemu dengan Menteri Pertahanan negara tersebut guna membahas peluang kerja sama teknologi militer serta penguatan *soldier-to-soldier contact*.⁵ Pertemuan ini kemudian ditindaklanjuti pada Agustus 2025 melalui kunjungan Kepala Departemen Pengembangan Peralatan Komisi Militer Pusat Republik Rakyat Tiongkok, Jenderal Xu Xieqiang, yang menjadi momentum penting dalam menegaskan komitmen kedua negara untuk mendorong kemandirian industri pertahanan nasional sekaligus meningkatkan daya saing global melalui skema alih teknologi.⁶

Selain Tiongkok, Indonesia juga aktif memperluas jejaring kerja sama teknologi pertahanan dengan mitra lain. Sepanjang 2025, Menteri Pertahanan Sjafrie dilaporkan melakukan sejumlah pertemuan dengan Menteri Pertahanan Jepang untuk membahas pertukaran teknologi militer, termasuk komitmen kerja sama dalam kerangka transfer teknologi dan penguatan kapasitas industri pertahanan nasional.⁷

Perkembangan kerja sama teknologi pertahanan yang dilakukan pemerintah dengan sejumlah negara tersebut perlu dibaca dalam konteks yang lebih luas. Seperti telah disinggung, penguatan teknologi pertahanan modern tidak hanya mencakup alutsista tradisional, tetapi juga instrumen persenjataan modern termasuk *spyware*. Terbukanya pintu bagi adopsi teknologi surveilans canggih ini berpotensi digunakan melampaui konteks pertahanan. Penggunaan *spyware* dapat menggeser batas antara kebutuhan pertahanan dan pelanggaran hak asasi manusia.

Perkembangan teknologi surveilans komersial telah menciptakan kesenjangan fundamental antara teknologi dengan regulasi hukum yang mengaturnya. Orinn Kerr

³ Kementerian Pertahanan Republik Indonesia, "Wamenhan RI Buka Defence Technology Forum 2025, Dorong Inovasi Teknologi Pertahanan," *Kemhan*, 19 November 2025, <https://www.kemhan.go.id/2025/11/19/wamenhan-ri-buka-defence-technology-forum-2025-dorong-inovasi-teknologi-pertahanan.html> (diakses pada 20 Januari 2026).

⁴ MetroTVNews, "Kemhan dan KNDS Jalin Kerja Sama Strategis di Bidang Teknologi," *MetroTVNews*, 20 November 2025, <https://www.metrotvnews.com/play/bD2CMewQ-kemhan-dan-knds-jalin-kerja-sama-strategis-di-bidang-teknologi> (diakses pada 20 Januari 2026).

⁵ Kementerian Pertahanan Republik Indonesia, "Menhan RI dan RRT Perkuat Kerja Sama Strategis Bidang Pertahanan," *Kemhan*, 22 Januari 2025, <https://www.kemhan.go.id/2025/01/22/menhan-ri-dan-rrt-perkuat-kerja-sama-strategis-bidang-pertahanan.html> (diakses pada 20 Januari 2026).

⁶ Sukarjito, "Prabowo Terima Jenderal China, Sepakat Perkuat Teknologi Militer," *BeritaSatu*, 6 Agustus 2025, <https://www.beritasatu.com/nasional/2910998/prabowo-terima-jenderal-china-sepakat-perkuat-teknologi-militer> (diakses pada 20 Januari 2026).

⁷ Antara News, "Menhan Bahas Kerja Sama Pertukaran Teknologi Militer dengan Jepang," *Antara News*, 7 Januari 2025, <https://www.antaranews.com/berita/4568354/menhan-bahas-kerja-sama-pertukaran-teknologi-militer-dengan-jepang> (diakses pada 20 Januari 2026).

menggambarkan fenomena ini sebagai situasi dimana “*the internet upends surveillance law*” yaitu sebuah kondisi arsitektur teknologi digital bergerak jauh lebih cepat daripada kemampuan sistem hukum secara global untuk mengantisipasi dan meresponnya.⁸ Dalam konteks *spyware* militer seperti Pegasus (NSO group) dan Predator (Intellexa) atau beberapa brand lainnya yang mengembangkan teknologi *spyware* sejenis, kesenjangan ini bukan hanya mengenai kelambanan hukum untuk merespon dan membuat pengaturan yang melindungi HAM, melainkan juga menimbulkan kesenjangan besar antara cara kerja hukum yang lama dengan kemampuan teknologi saat ini.⁹

Lompatan Kemampuan *Spyware*: Dari Intersepsi Komunikasi ke Zero Click

Spyware generasi terbaru memiliki karakteristik yang secara fundamental berbeda. Pegasus dapat menginfeksi perangkat tanpa memerlukan interaksi pengguna seperti metode lawas yang umumnya berisi link phishing dan pengguna harus mengklik link atau mendownload file (*zero click exploitation*). Setelah terinstal, *spyware* generasi baru saat ini langsung memberikan akses penuh ke seluruh fungsi perangkat mulai dari kamera, mikrofon, gps, bahkan aplikasi terenkripsi seperti WhatsApp dan Signal, termasuk data yang telah dihapus. Operasinya tidak meninggalkan jejak yang dapat dideteksi oleh pengguna ataupun antivirus komersil yang banyak beredar. Ketika perangkat sudah terjangkit maka *spyware* dapat tetap aktif dalam jangka waktu tidak terbatas tanpa memerlukan akses fisik ke perangkat.¹⁰

Dalam perspektif hak asasi manusia, tingkat intrusi ini melampaui konsep penggeledahan menyeluruh yang dikenal dalam hukum pidana. Karena ia mengubah *device* (smartphone/laptop/komputer) menjadi alat pengawasan permanen yang bekerja tanpa batas ruang dan waktu, memungkinkan negara atau aktor pengguna untuk mengakses secara berkelanjutan kehidupan privat seseorang bahkan ke tahap paling privat.

Karakteristik teknis ini menantang asumsi dasar dalam hukum surveilans yang ada, yang dirancang untuk era di mana penyadapan memerlukan akses fisik atau setidaknya meninggalkan jejak yang dapat dideteksi. Dalam konteks hukum Indonesia, tidak ada satu pun undang-undang yang secara spesifik mengatur teknologi dengan kemampuan seperti ini. Terdapat kekosongan hukum yang berbahaya.

Investigasi Citizen Lab di 2021 mengungkap bahwa Pegasus telah digunakan di 45 negara untuk menyerang jurnalis, aktivis HAM, pengacara, dan oposisi politik.¹¹

⁸ Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie K. Pell, “It’s Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law,” *Harvard Journal of Law & Technology*, volume 30, nomor 1, 2016, halaman 2-73.

⁹ *Ibid.*

¹⁰ George Packer, “How Democracies Spy on Their Citizens,” *The New Yorker*, 25 April 2022, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens> (diakses pada 20 Januari 2026).

¹¹ Forbidden Stories, “Pegasus: The New Global Weapon for Silencing Journalists,” *ForbiddenStories.org*, April 2022, <https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/> (diakses pada 20 Januari 2026).

Sebelumnya di tahun 2019 dalam kasus WhatsApp v NSO Group. Terungkap fakta bahwa *spyware* ini telah menjangkiti 1.223 pengguna WhatsApp di 51 negara, termasuk Indonesia dengan 54 nomor yang menjadi korban.¹² Berdasarkan data ini WhatsApp menggugat NSO Group atas tuduhan pelanggaran privasi massal. Hingga hari ini berbagai penyalahgunaan Pegasus terus berlanjut di berbagai belahan dunia. Pada Oktober 2024, terungkap pemerintah Polandia menggunakan *spyware* ini untuk mematai aktivis hak perempuan. Tindakan serupa dijumpai di beberapa negara Eropa lainnya termasuk Yunani dan Spanyol. Temuan paling baru juga menunjukkan serangan di Februari 2025 dengan korban dua orang editor Balkan Investigative Reporting Network.¹³

Kerangka Hukum Indonesia, *Safeguard*, dan Prinsip Internasional

Di Indonesia, kerangka regulasi yang ada baik dalam UU ITE, UU Intelijen, maupun UU Perlindungan Data Pribadi, masih belum mampu beradaptasi dalam mengatur penggunaan *spyware* secara memadai. Ketiga regulasi ini jauh tertinggal secara perkembangan teknologi, disaat bersamaan berbagai pasal “karet” di dalamnya membuka ruang legitimasi bagi surveilans yang dilakukan tanpa mekanisme pengawasan yang efektif.

Merujuk pada tiga instrumen hukum Indonesia saat ini terlihat pola kelemahan yang konsisten, yaitu ketiadaan *safeguard* untuk surveilans jauh di bawah standar internasional. Kekurangan ini bukan hanya di aspek gagap teknologi, namun juga dalam struktur sistem *check and balances* yang memadai untuk membatasi kekuasaan negara atau aktor lainnya dalam melakukan surveilans terhadap warga negara.

Dengan kata lain, persoalan *spyware* di Indonesia bukan sekadar soal kekosongan norma hukum, melainkan juga lemahnya mekanisme pengawasan demokratis yang seharusnya menjadi prasyarat utama dalam setiap tindakan pengawasan. Dalam teori ketatanegaraan, surveilans harus tunduk pada kontrol parlemen, otorisasi pengadilan, serta pengawasan lembaga independen. Namun dalam praktiknya, *spyware* justru beroperasi dalam ruang minim akuntabilitas karena sifatnya yang rahasia, invasif, dan hampir selalu dibenarkan melalui narasi keamanan nasional.

Kelemahan struktural ini tercermin secara nyata dalam kerangka hukum yang ada saat ini baik melalui UU ITE yang menormalisasi praktik patroli siber tanpa definisi dan batasan jelas, UU Intelijen yang memberikan kewenangan luas tanpa kontrol yudisial, maupun UU Perlindungan Data Pribadi yang membuka pengecualian keamanan nasional secara elastis. Ketiga instrumen tersebut menunjukkan pola yang sama: perluasan

¹² VSquare.org, “Pegasus Spyware Hacking WhatsApp – Meta, Hungary, Czech Republic,” VSquare.org, 17 April 2025, <https://vsquare.org/pegasus-spyware-hacking-whatsapp-meta-hungary-czech-republic/> (diakses pada 20 Januari 2026).

¹³ *Ibid.*

kewenangan surveilans tidak diimbangi dengan safeguard, transparansi, maupun mekanisme pemulihan bagi korban.

UU ITE dan Normalisasi Patroli Siber

Merujuk UU ITE dalam praktik yang terdokumentasi kerap dijadikan dasar normatif untuk model patroli siber, pemantauan digital yang dapat berujung pada pengawasan lebih lanjut, penyidikan, hingga penangkapan. Lewat pola operasional patroli siber yang teridentifikasi bergerak dari pemantauan konten, lalu pendalaman lebih lanjut terhadap target, data ini dapat digunakan sebagai dasar proses hukum. Sayangnya dalam UU ITE tidak ada definisi legal mengenai operasi patroli siber ataupun terkait penyadapan dan surveilans itu sendiri, batasan data yang diperbolehkan untuk diakses dan dikumpulkan, dan tentunya tidak ada mekanisme pengawasan independen untuk memastikan *check and balance* dalam prosesnya. Secara definitif, penyadapan di Indonesia sejauh ini diatur melalui KUHP Baru di pasal 258 ayat (1).

"Setiap Orang yang secara melawan hukum mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, dipidana dengan pidana penjara paling lama 10 tahun atau pidana denda paling banyak kategori VI, yaitu pidana denda paling banyak 2 Miliar rupiah."

Namun, definisi ini tidak mencakup kemampuan *spyware* modern yang melampaui "penyadapan" tradisional. Kritik utama terhadap kerangka hukum ini adalah bahwa ia dirancang untuk era di mana surveilans memerlukan tindakan aktif dan dapat dideteksi, bukan untuk teknologi yang dapat beroperasi secara diam-diam dan permanen melalui teknologi *spyware* seperti saat ini.

UU Intelijen dan Ketiadaan Pengawasan Yudisial

Dalam konteks UU Intelijen otorisasi surveilans dapat bergerak melalui mekanisme internal atau izin tertulis dari pejabat/presiden yang pada prinsipnya tidak memenuhi standar *independent oversight* ketika tindakan negara dapat mengakses seluruh aspek kehidupan privat. Ini berbeda secara mendasar dengan mekanisme penyadapan dalam konteks penegakan hukum pidana umum, di mana KUHP dan UU Pemberantasan Tindak Pidana Korupsi mensyaratkan izin pengadilan untuk penyadapan, meskipun dengan pengecualian untuk kasus-kasus tertentu seperti korupsi tingkat tinggi, terorisme, dan narkoba yang dapat dilakukan tanpa izin pengadilan terlebih dahulu namun harus dilaporkan kepada pengadilan dalam waktu tertentu.

Dalam konteks intelijen dan keamanan nasional, bahkan mekanisme pelaporan pasca-tindakan pun tidak ada, sehingga surveilans dapat dilakukan sepenuhnya tanpa kontrol yudisial. Penjelasan Pasal 32 (1) UU Intelijen mendefinisikan penyadapan sebagai:

"kegiatan mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetik atau radio frekuensi, termasuk memeriksa paket, pos, surat-menyurat, dan dokumen lain."

Definisi penyadapan tersebut belum mencakup surveilans menggunakan teknologi yang modern.

Selain itu, UU Intelijen juga memberikan kewenangan luas tanpa mekanisme pengawasan yang memadai. Dalam praktik, ini berarti bahwa lembaga intelijen dapat melakukan surveilans terhadap siapa pun yang dianggap sebagai "ancaman keamanan nasional" tanpa harus membuktikan kepada otoritas independen bahwa tindakan tersebut *necessary* dan *proportionate*.

Perbandingan dengan praktik negara demokratis lain memperjelas kelemahan pengaturan surveilans di Indonesia. Amerika Serikat memiliki US Foreign Intelligence Surveillance Court, sebuah pengadilan khusus yang harus memberikan izin untuk setiap surveilans dalam konteks keamanan nasional.¹⁴ Meskipun sistem ini tidak sempurna dan sering dikritik karena tingkat penolakan yang rendah dan kurangnya transparansi, setidaknya ada mekanisme pengawasan yudisial yang dapat diaudit dan direview oleh lembaga pengawas independen seperti Privacy and Civil Liberties Oversight Board.¹⁵

UU PDP dan Pengecualian Keamanan Nasional

Pengesahan Undang-Undang Pelindungan Data Pribadi (UU PDP) pada 2022 ditujukan untuk melindungi data pribadi warga negara. Namun UU ini masih menyisakan ruang abu-abu yang memberi ruang pada tindakan pelanggaran data pribadi. Hal ini terdapat dalam Pasal 15 ayat 1 (1) yang menyatakan bahwa hak subjek data pribadi dikecualikan untuk: a. kepentingan pertahanan dan keamanan nasional; b. kepentingan proses penegakan hukum. Kedua pasal ini memberikan pengecualian untuk kepentingan tertentu, termasuk keamanan nasional dan penegakan hukum, tanpa indikator yang jelas. Dalam praktiknya, pengecualian ini dapat diinterpretasikan secara elastis untuk mencakup hampir semua aktivitas surveilans yang dilakukan oleh lembaga keamanan dan intelijen.

Meskipun pengecualian atas dasar penegakan hukum atau keamanan nasional dalam situasi tertentu dapat dibenarkan, ketiadaan batasan yang tegas serta mekanisme pengawasan yang transparan membuat pengecualian tersebut sangat rentan

¹⁴ American Civil Liberties Union (ACLU), "Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress," *ACLU.org*, 11 April 2023, <https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress> (diakses pada 20 Januari 2026).

¹⁵ Brennan Center for Justice, "Privacy and Civil Liberties Oversight Board Embraces Surveillance Reforms," *BrennanCenter.org*, 11 Oktober 2023, <https://www.brennancenter.org/our-work/analysis-opinion/privacy-and-civil-liberties-oversight-board-embraces-surveillance-reforms> (diakses pada 20 Januari 2026).

disalahgunakan. Merujuk sejumlah peristiwa yang pernah terjadi, dalih keamanan nasional kerap dipakai untuk melegitimasi praktik pengawasan yang serampangan (*indiscriminate*) dan massal.

Sebagai contoh, Investigatory Powers Tribunal (IPT) di Inggris pernah memutuskan bahwa akses badan intelijen Inggris (GCHQ) terhadap komunikasi pribadi yang dikumpulkan secara besar-besaran oleh National Security Agency (NSA) melanggar hukum HAM, khususnya hak atas privasi dan kebebasan berekspresi. Praktik pertukaran data intelijen dalam skala industri tersebut dinilai ilegal karena dilakukan tanpa kerangka pengawasan publik yang memadai.¹⁶

Dalam konteks penggunaan *spyware*, pengecualian serupa dapat menjadi sangat problematik apabila digunakan untuk membenarkan surveilans massal terhadap tersangka, atau bahkan individu yang sekadar dicurigai tanpa bukti yang cukup. Kondisi ini pada akhirnya membuka jalan bagi pelanggaran HAM sistemik, sebagaimana telah terjadi dalam praktik pengawasan global sebelumnya.¹⁷

Berbeda dengan pendekatan yang kerap memberi ruang luas bagi dalih keamanan nasional tanpa kontrol yang memadai, kerangka Uni Eropa melalui GDPR justru menempatkan pengecualian tersebut dalam rezim pembatasan yang ketat dan diawasi secara independen. Pasal 23 GDPR memang membuka kemungkinan bagi negara anggota untuk membatasi hak-hak subjek data demi tujuan seperti keamanan nasional atau keamanan publik. Namun pembatasan ini tidak bersifat otomatis atau blanket exemption, melainkan hanya dapat dibenarkan apabila ditetapkan melalui hukum yang jelas, tetap menghormati esensi hak-hak fundamental, serta memenuhi uji *necessity* dan *proportionality* dalam masyarakat demokratis, disertai safeguard yang memadai.¹⁸

Lebih jauh, GDPR juga menegaskan bahwa bahkan ketika negara mengklaim pengecualian berbasis keamanan, penerapannya tetap harus berada dalam pengawasan lembaga independen. Chapter VI (Articles 51–54) mewajibkan setiap negara anggota membentuk *supervisory authority* yang independen, dengan mandat dan kewenangan nyata untuk memantau pelaksanaan regulasi, termasuk menilai legitimasi derogasi atau pembatasan hak.¹⁹ Prinsip independensi ini krusial karena memastikan pengawasan tidak berada di bawah kendali langsung negara atau aparat keamanan itu sendiri. Dengan demikian, GDPR menunjukkan bahwa keamanan nasional tidak dapat dijadikan

¹⁶ Amnesty International UK, “UK Government GCHQ Mass Spying Surveillance,” *Amnesty.org.uk*, 1 April 2025, <https://www.amnesty.org.uk/knowledge-hub/all-resources/uk-government-gchq-ipt-mass-spying-surveillance/> (diakses pada 20 Januari 2026).

¹⁷ Pieter Omtzigt, Mass Surveillance, Report, Doc. 13734 (Strasbourg: Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, 8 Maret 2015).

¹⁸ European Data Protection Board, Guidelines 10/2020 on Restrictions under Article 23 GDPR, version 2.0 (Brussels: EDPB, Oktober 2021), paras. 37–40.

¹⁹ Regulation (EU) 2016/679 (GDPR), arts. 51–54 (Chapter VI: Independent Supervisory Authorities), OJ L 119 (4 Mei 2016).

pembenaran untuk surveilans massal tanpa batas, melainkan harus tunduk pada kontrol hukum, prinsip proporsionalitas, dan mekanisme akuntabilitas eksternal.

Pembelajaran dari yurisdiksi yang sudah ada, menunjukkan bahwa pengecualian keamanan nasional dalam undang-undang perlindungan data sering kali menjadi pintu masuk untuk surveilans yang melanggar HAM. Dalam kasus *Roman Zakharov v. Russia* (2015), European Court of Human Rights (ECtHR) memutuskan bahwa pengecualian keamanan nasional dalam hukum Rusia yang memungkinkan surveilans tanpa pengawasan yudisial yang memadai melanggar Pasal 8 European Convention on Human Rights tentang hak atas privasi.²⁰ Pengadilan menekankan bahwa meskipun keamanan nasional adalah kepentingan yang sah, surveilans harus tetap memenuhi standar *necessity* dan *proportionality* serta tunduk pada pengawasan independen.

Demikian pula, dalam kasus *Big Brother Watch and Others v. United Kingdom* (2018), ECtHR memutuskan bahwa rezim surveilans massal Inggris melanggar hak atas privasi karena tidak memiliki safeguard yang memadai, termasuk oversight independen dan mekanisme notifikasi kepada individu yang menjadi target surveilans.²¹ Putusan ini menegaskan bahwa pengecualian keamanan nasional tidak dapat digunakan sebagai justifikasi untuk surveilans tanpa batas.

Terkait dengan hak notifikasi, ECtHR juga telah memberikan standar yang jelas dalam kasus *Ekimdziev v. Bulgaria* (2007). Dalam putusan tersebut, ECtHR menetapkan bahwa setelah surveilans berakhir dan waktu yang singkat untuk mencapai tujuan legitimasi dari surveilans telah berlalu, notifikasi kepada individu yang terkena dampak harus dilakukan tanpa penundaan (*without delay*).²² Pengadilan menekankan bahwa hak untuk diberitahu tentang surveilans adalah komponen esensial dari hak atas pemulihan yang efektif (*effective remedy*), karena tanpa notifikasi, individu tidak akan pernah mengetahui bahwa hak privasi mereka telah dilanggar dan tidak akan dapat menggugat legalitas tindakan surveilans tersebut.

Standar Ekimdziev ini kemudian diperkuat dalam berbagai putusan ECtHR selanjutnya, termasuk dalam kasus *Weber and Saravia v. Germany* (2006)²³ dan *Liberty and Others v. United Kingdom* (2008),²⁴ yang menekankan bahwa sistem surveilans yang tidak memiliki

²⁰ European Court of Human Rights (Grand Chamber), *Roman Zakharov v. Russia* (Application no. 47143/06), Judgment, 4 Desember 2015, <https://hudoc.echr.coe.int/fre?i=001-159324> (diakses pada 20 Januari 2026).

²¹ European Court of Human Rights (Grand Chamber), *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14, and 24960/15), Judgment, 25 Mei 2021, <https://hudoc.echr.coe.int/fre?i=001-210077> (diakses pada 20 Januari 2026).

²² European Court of Human Rights (Fifth Section), *Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria* (Application no. 62540/00), Judgment, 28 Juni 2007, <https://hudoc.echr.coe.int/eng?i=001-81323> (diakses pada 20 Januari 2026).

²³ European Court of Human Rights (Chamber), *Weber v. Switzerland* (Application no. 11034/84), Judgment, 22 Mei 1990, <https://hudoc.echr.coe.int/eng?i=001-57629> (diakses pada 20 Januari 2026).

²⁴ European Court of Human Rights (Fourth Section), *Liberty and Others v. the United Kingdom* (Application no. 58243/00), Judgment, 1 Juli 2008, <https://hudoc.echr.coe.int/eng?i=001-87207> (diakses pada 20 Januari 2026).

mekanisme notifikasi yang memadai secara inheren melanggar Pasal 8 European Convention on Human Rights (ECHR). ECtHR secara konsisten menyatakan bahwa meskipun penundaan notifikasi dapat dibenarkan dalam kasus-kasus tertentu untuk melindungi investigasi yang sedang berlangsung, penundaan tersebut harus dibatasi secara ketat dan harus ada mekanisme untuk memastikan bahwa notifikasi akhirnya akan dilakukan

Di Indonesia, ketiadaan safeguard dalam UU PDP untuk surveilans yang dilakukan atas nama keamanan nasional menciptakan risiko yang sangat serius. Tanpa mekanisme pengawasan independen, tidak ada cara untuk memastikan bahwa surveilans yang dilakukan oleh lembaga keamanan dan intelijen memenuhi standar *necessity* dan *proportionality*. Tanpa kewajiban notifikasi kepada individu yang menjadi target, tidak ada cara bagi korban surveilans untuk mengetahui bahwa mereka telah diawasi dan untuk menggugat legalitas tindakan tersebut

Lebih jauh lagi, UU PDP tidak mengatur secara spesifik tentang penggunaan teknologi surveilans yang invasif seperti *spyware*. Meskipun Pasal 20 UU PDP mengatur tentang kewajiban pengendali data pribadi untuk melindungi data pribadi dari akses yang tidak sah, ketentuan ini tidak berlaku untuk surveilans yang dilakukan oleh negara atas nama keamanan nasional karena pengecualian di Pasal 15 ayat 1(1). Ini berarti bahwa penggunaan *spyware* oleh lembaga keamanan dan intelijen untuk mengakses data pribadi warga negara tidak tunduk pada ketentuan perlindungan data pribadi sama sekali.

Kritik terhadap kerangka hukum ini semakin relevan ketika dikaitkan dengan temuan Citizen Lab (2023) yang mengidentifikasi penggunaan Pegasus di Indonesia. Dalam kondisi UU PDP yang memberikan pengecualian luas atas dasar keamanan nasional tanpa *safeguard* yang jelas, tidak tersedia mekanisme hukum yang efektif untuk menilai apakah penggunaan *spyware* dilakukan secara legal, untuk tujuan yang sah, serta dengan cara yang *necessary* dan *proportionate*. Ketidadaan transparansi dan akuntabilitas ini menciptakan ruang gelap yang memungkinkan *spyware* digunakan bukan untuk perlindungan publik, melainkan untuk memantau oposisi politik, jurnalis, atau aktivis HAM.

Risiko tersebut tidak bersifat hipotetis. Pengalaman Amerika Latin menunjukkan bagaimana pengecualian keamanan nasional dalam rezim perlindungan data sering kali berubah menjadi alat legitimasi bagi praktik surveilans yang melanggar HAM, terutama ketika negara juga membangun infrastruktur pemantauan digital melalui aparat keamanan dan unit patroli siber. Laporan AISur (2025) mendokumentasikan bahwa di Meksiko, penggunaan Pegasus oleh SEDENA untuk memata-matai jurnalis dan pembela HAM dilakukan di luar jangkauan ketentuan perlindungan data, karena diklaim sebagai

bagian dari mandat keamanan nasional.²⁵ Di Brasil, penggunaan *spyware* FirstMile oleh badan intelijen ABIN pada era Bolsonaro juga berlangsung tanpa kontrol hukum yang memadai dengan justifikasi serupa.²⁶

Pola ini menunjukkan bahwa ketika negara memiliki kapasitas teknis untuk surveilans, melalui *spyware* maupun patroli siber namun pengecualian hukum dibiarkan terlalu luas, maka perlindungan data kehilangan fungsi dasarnya sebagai instrumen pembatas kekuasaan. Situasi Indonesia mencerminkan kecenderungan yang sama: pengecualian keamanan nasional dalam UU PDP berpotensi menciptakan “zona bebas hukum” yang memungkinkan pengawasan digital invasif tanpa mekanisme *check and balance*.

Lemahnya *Check and Balances* dalam Pengawasan Digital: *spyware* sebagai Zona Bebas Akuntabilitas

Dalam negara hukum, tindakan surveilans tidak dapat diperlakukan sebagai diskresi aparat semata, melainkan harus tunduk pada prinsip *legality*, *necessity*, dan *proportionality*, disertai mekanisme *check and balances* yang efektif. Tanpa pengawasan independen, *spyware* beroperasi sebagai bentuk kekuasaan tersembunyi (*hidden power*) yang mampu mengakses kehidupan privat warga negara secara total, tanpa kontrol publik maupun pemulihan yang memadai.

Dalam konteks Indonesia, persoalan *check and balances* ini menjadi lebih krusial karena *spyware* hampir selalu dibenarkan melalui narasi keamanan nasional. Ketika suatu tindakan pengawasan diklaim sebagai bagian dari “pertahanan negara” atau “ancaman keamanan”, ruang kritik dan kontrol demokratis mengecil secara drastis. Akibatnya, *spyware* berpotensi menciptakan rezim surveilans yang tidak hanya melanggar hak atas privasi, tetapi juga mengancam kebebasan berekspresi, kebebasan berserikat, serta partisipasi politik dalam demokrasi.

Secara formal, DPR khususnya Komisi I memiliki mandat pengawasan terhadap sektor pertahanan dan intelijen melalui fungsi legislasi, anggaran, dan kontrol politik.²⁷ Namun dalam praktiknya, pengawasan parlemen terhadap teknologi surveilans sering kali bersifat simbolik dan terbatas. Belanja pertahanan dan keamanan, termasuk perangkat pengawasan digital, kerap ditempatkan dalam pos-pos anggaran yang tertutup karena masuk ke ranah rahasia negara.

Di sisi lain pengawasan yudisial seharusnya menjadi *safeguard* utama dalam membatasi surveilans belum memiliki kerangka prosedural maupun kapasitas institusional untuk melakukan tinjauan substantif terhadap *spyware* ataupun aktivitas surveilans yang

²⁵ Silvia Calderón dan Ana Gaitán, eds., *Surveillance Trends and Practices in Latin America: Case Studies from Brazil, Chile, Colombia, El Salvador, Mexico, Peru, and Paraguay* (Juni 2025).

²⁶ *Ibid.*

²⁷ Indonesia Baik, “Bidang Kerja 13 Komisi DPR RI Periode 2024–2029,” *Indonesiabaik.id*, 2017, <https://indonesiabaik.id/infografis/bidang-kerja-13-komisi-dpr-ri-periode-2024-2029> (diakses pada 3 Februari 2026)

dilakukan. Tidak terdapat mekanisme khusus seperti *surveillance court* yang dapat menguji apakah suatu operasi *spyware* benar-benar memenuhi prinsip *necessity* dan *proportionality*. Lebih jauh, rezim intelijen dan keamanan nasional justru memungkinkan surveilans dilakukan melalui otorisasi internal tanpa surat perintah ataupun pengawasan pengadilan.

Dalam negara demokratis, mekanisme ini merupakan *safeguard* krusial karena penyalahgunaan *spyware* sering kali tidak terdeteksi pada tahap otorisasi awal, terutama ketika operasi dilakukan secara rahasia. Model pengawasan semacam ini dijalankan oleh lembaga independen seperti Privacy and Civil Liberties Oversight Board (PCLOB) di Amerika Serikat atau Inspector-General of Intelligence and Security (IGIS) di Australia, yang memiliki kewenangan mengaudit operasi surveilans secara berkala, mengakses dokumen rahasia negara, serta menilai apakah tindakan tersebut memenuhi prinsip *necessity and proportionality* serta tidak melanggar HAM target surveilans. Lembaga ini juga berwenang menjatuhkan rekomendasi penghentian operasi, pemusnahan data ilegal, hingga sanksi terhadap pejabat yang menyalahgunakan kewenangan.

Hingga saat ini Indonesia belum memiliki lembaga pengawas untuk operasi surveilans, kecuali mekanisme internal yang sifatnya tertutup. Akibatnya, penyalahgunaan *spyware* hampir tidak mungkin diketahui oleh korban yang haknya dilanggar atau oleh publik. Kondisi ini menunjukkan bahwa *spyware* beroperasi dalam ruang minim akuntabilitas struktural. Dalam lanskap seperti ini, pengaturan *spyware* tidak cukup hanya melalui norma hukum, tetapi mensyaratkan reformasi institusional yang menempatkan pengawasan independen sebagai prasyarat.

Kesenjangan antara Hukum dan Teknologi: Kegagalan Mengatur *Spyware*

Kerangka hukum Indonesia masih menghadapi kesenjangan fundamental dalam mengatur *spyware*. Kesenjangan ini tampak dalam beberapa hal berikut: Pertama, definisi "penyadapan" dalam berbagai undang-undang masih mengacu pada konsep tradisional yang tidak mencakup kemampuan *spyware* modern. Kedua, tidak ada undang-undang yang secara spesifik mengatur tentang akuisisi, pengoperasian, dan penggunaan *spyware* oleh negara. Ketiga, tidak ada mekanisme *check and balance* yang dapat mengawasi penggunaan teknologi surveilans yang invasif.

Hukum surveilans tradisional dirancang berdasarkan asumsi bahwa surveilans memerlukan tindakan fisik yang dapat dideteksi dan dibatasi. Namun, teknologi digital, khususnya *spyware*, mengubah asumsi ini secara fundamental.²⁸ *Spyware* dapat beroperasi secara diam-diam, tanpa meninggalkan jejak, dan memberikan akses yang jauh lebih invasif daripada penyadapan tradisional sehingga hukum yang dirancang

²⁸ Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie K. Pell, "It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law," *Harvard Journal of Law & Technology* Volume 30, Nomor 1, 2016, halaman 2-73.

untuk era analog tidak mampu mengatur teknologi digital yang beroperasi dengan logika yang berbeda.²⁹

Dalam konteks Indonesia, kelemahan ini semakin diperparah oleh ketiadaan transparansi tentang pengadaan dan penggunaan *spyware*. Terdapat rantai birokrasi yang panjang dan “gelap” untuk pengadaan alat-alat pertahanan dan keamanan. Selain itu tidak ada mekanisme hukum yang mewajibkan lembaga keamanan dan intelijen untuk mengungkapkan apakah mereka menggunakan *spyware*, untuk tujuan apa, dan terhadap siapa. Hal ini juga diperparah dengan rapat-rapat dan pertemuan di Komisi 1 DPR RI sebagai pengawas pemerintah kerap kali diadakan secara tertutup sehingga publik sulit untuk memantau pengadaan dan evaluasinya. Fenomena ini terjadi secara global, bahwa tanpa kerangka hukum yang spesifik untuk mengatur *spyware*, teknologi ini akan digunakan secara tidak terkontrol dan melanggar HAM. Di Israel, meskipun NSO Group beroperasi di bawah lisensi ekspor yang dikeluarkan oleh Kementerian Pertahanan, tidak ada mekanisme pengawasan domestik yang mengawasi bagaimana Pegasus digunakan oleh negara-negara klien sehingga Pegasus telah digunakan untuk menyerang jurnalis, aktivis HAM, dan oposisi politik di puluhan negara.³⁰

Di Uni Eropa, beberapa negara telah mulai didorong untuk mengembangkan kerangka hukum yang spesifik untuk mengatur *spyware*. Pada 2019 Special Rapporteur UN untuk Kebebasan Berpendapat dan Berekspresi, merekomendasikan moratorium terhadap penjualan, transfer, dan penggunaan teknologi surveilans sampai kerangka peraturan yang sesuai dengan perlindungan HAM diberlakukan.³¹ Rekomendasi ini dituangkan dalam laporannya mengenai industri surveilans dan gangguannya terhadap HAM. Dalam laporannya ia menulis “*Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control.*” Melalui laporan ini setiap negara didesak untuk mengadopsi perlindungan domestik sesuai dengan hukum HAM Internasional untuk melindungi individu ataupun kelompok dari surveilans yang melanggar hukum.³²

Pada 2022, Parlemen Eropa membentuk komite khusus PEGA Committee (Komite Pegasus) untuk menyelidiki penggunaan Pegasus dan *spyware* lainnya di negara-negara

²⁹ *Ibid.*

³⁰ Organized Crime and Corruption Reporting Project (OCCRP), “Where NSO Group Came From and Why It’s Just the Tip of the Iceberg,” *The Pegasus Project*, 20 Juli 2021, <https://www.occrp.org/en/project/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg> (diakses pada 20 Januari 2026).

³¹ United Nations Human Rights Council, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/41/35, 41st sess. 24 June–12 July 2019, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur> (diakses pada 20 Januari 2026)

³² *Ibid.*

anggota Uni Eropa.³³ Komite ini menemukan bahwa *spyware* telah digunakan secara melanggar hukum di beberapa negara, termasuk Polandia, Hungaria, Yunani, dan Spanyol, untuk memata-matai jurnalis, pengacara, dan politisi oposisi.³⁴ Sebagai respons, Parlemen Eropa merekomendasikan moratorium penggunaan *spyware* hingga ada kerangka hukum yang memadai untuk mengaturnya

Temuan PEGA Committee sangat mengkhawatirkan karena menunjukkan bahwa bahkan di negara-negara dengan tradisi demokrasi yang kuat dan kerangka hukum HAM yang mapan, *spyware* dapat disalahgunakan untuk tujuan politik. Di Polandia, misalnya, komite menemukan bahwa pemerintah menggunakan Pegasus untuk memata-matai lebih dari 600 individu, termasuk senator oposisi, pengacara yang menangani kasus-kasus sensitif secara politik, dan jurnalis investigatif.³⁵ Penggunaan ini dilakukan tanpa otorisasi yudisial yang memadai dan tanpa notifikasi kepada korban. Walaupun Polandia akhirnya mengakui penggunaan Pegasus, namun terdapat bantahan bahwa alat ini digunakan untuk memata-matai lawan politik.³⁶

Di Hungaria, investigasi mengungkapkan bahwa pemerintah Viktor Orbán menggunakan Pegasus untuk memata-matai. Setidaknya ditemukan lebih dari 300 nomor telepon yang terindikasi disusupi Pegasus.³⁷ Nomor-nomor yang diawasi tersebut di antaranya milik politisi, pengacara, serta jurnalis investigatif, termasuk mereka yang bekerja untuk Direkt36 dan Átlátszó, dua outlet media independen yang sering mengkritik pemerintah. Dalam beberapa kasus, infeksi Pegasus terjadi tepat sebelum publikasi investigasi penting tentang korupsi pemerintah, menunjukkan bahwa surveilans digunakan untuk mengintimidasi jurnalis dan menggagalkan investigasi korban.³⁸

Di Yunani, skandal Predator Gate pada tahun 2022 mengungkapkan bahwa pemerintah menggunakan *spyware* Predator (diproduksi oleh Intellexa, perusahaan yang berbasis di Yunani) untuk memata-matai jurnalis investigatif Thanasis Koukakis dan politisi oposisi Nikos Androulakis.³⁹ Skandal ini berujung pengunduran diri kepala intelijen Yunani yang

³³ European Parliament, "Parliament Establishes Inquiry Committee," *European Parliament Committees*, 16 August 2022, <https://www.europarl.europa.eu/committees/en/parliament-establishes-inquiry-committee/product-details/20220816CHE10529> (diakses pada 20 Januari 2026).

³⁴ European Parliament, Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2022/2077(INI))*, Rapporteur Sophie in 't Veld, 22 May 2023 (diakses pada 20 Januari 2026).

³⁵ *Ibid.*

³⁶ Deutsche Welle (DW), "Poland Top Leader Admits Government Bought Pegasus Spyware," *DW*, 27 Desember 2021, <https://www.dw.com/en/poland-top-leader-admits-government-bought-pegasus-spyware/a-60361211> (diakses pada 20 Januari 2026).

³⁷ European Parliament, Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2022/2077(INI))*, Rapporteur Sophie in 't Veld, 22 May 2023 (diakses pada 20 Januari 2026).

³⁸ *Ibid.*

³⁹ European Parliamentary Research Service (EPRS), *Greece's Predatorgate: The Latest Chapter in Europe's Spyware Scandal?*, Briefing Paper,

juga mengakui penggunaan *spyware*, hal ini memicu debat nasional tentang perlunya regulasi yang lebih ketat terhadap *spyware*.⁴⁰

Investigasi ini menghasilkan rekomendasi yang difinalkan pada 15 Juni 2023. Rekomendasi ini muncul sebagai respons atas bukti bahwa perangkat pengawasan digunakan untuk memantau, memeras, dan mengintimidasi kelompok oposisi, para pengkritik, serta masyarakat sipil.⁴¹ Rekomendasi yang disusun termasuk menyerukan pemberlakuan moratorium segera terhadap penjualan, pembelian, pemindahan, dan penggunaan *spyware*, terutama bagi negara-negara yang belum memenuhi persyaratan ketat dan spesifik. Dengan syarat moratorium hanya dapat dicabut apabila (1) Semua dugaan penyalahgunaan *spyware* telah diselidiki secara menyeluruh; (2) Negara terkait menyetujui proses investigasi, termasuk yang diusulkan oleh Komite; (3) Tersedia kerangka hukum yang jelas, transparan, dan memastikan penggunaan yang bertanggung jawab; (4) Seluruh izin ekspor yang tidak sesuai dengan regulasi Uni Eropa dicabut.⁴²

Rekomendasi ini mencerminkan pengakuan bahwa *spyware* merepresentasikan ancaman yang sangat serius terhadap demokrasi dan HAM, dan bahwa kerangka hukum yang ada tidak memadai untuk mengaturnya. Indonesia perlu memperhatikan pelajaran dari pengalaman Uni Eropa ini dan mengembangkan kerangka hukum yang komprehensif sebelum penggunaan *spyware* menjadi lebih meluas.

Ketentuan dan Prosedur Pemantauan Komunikasi

Bahkan dengan pembatasan yang jelas tentang siapa yang dapat menggunakan *spyware* dan dalam kasus apa, risiko penyalahgunaan tetap tinggi mengingat sifat invasif teknologi ini. Terlebih masih belum ada kesepakatan bersama apakah *spyware* dapat dikategorikan sebagai alat strategis militer atau hanya dianggap sebagai pendukung dalam operasi militer. Oleh karena itu, kerangka hukum harus mencakup *safeguard* untuk mencegah, mendeteksi, dan memperbaiki penyalahgunaan. *Safeguard* ini idealnya dibangun di atas fondasi normatif internasional yang telah diakui secara luas, khususnya "International Principles on the Application of Human Rights to Communications Surveillance" atau Prinsip Necessary and Proportionate yang dikembangkan oleh koalisi organisasi masyarakat sipil global pada tahun 2013 dan telah diadopsi sebagai rujukan oleh berbagai badan HAM internasional, termasuk UN Special Rapporteur on Privacy,

2022, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA\(2022\)733637_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf) (diakses pada 20 Januari 2026).

⁴⁰ Deutsche Welle (DW), "Greece Spy Chief Quits Amid Predator Spyware Furor," DW, 5 Agustus 2022, <https://www.dw.com/en/greece-spy-chief-quits-amid-predator-spyware-furor/a-62723640> (diakses pada 20 Januari 2026).

⁴¹ Progressive Alliance of Socialists and Democrats in the European Parliament (S&D), "Pegasus Spyware Inquiry: S&Ds Call for Strong EU Regulation to Prevent Abuse by Member States," *Socialists and Democrats*, 14 Juni 2023, <https://www.socialistsanddemocrats.eu/newsroom/pegasus-spyware-inquiry-sds-call-strong-eu-regulation-prevent-abuse-member-states> (diakses pada 20 Januari 2026).

⁴² *Ibid.*

UN Special Rapporteur on Freedom of Expression, dan Inter-American Commission on Human Rights.⁴³

Secara global, tanpa adanya *safeguard* yang memadai, bahkan negara-negara dengan tradisi demokrasi yang kuat dapat mengalami penyalahgunaan *spyware* yang serius. Investigasi PEGA Committee di Parlemen Eropa maupun temuan berbagai lembaga masyarakat sipil di berbagai belahan dunia menunjukkan pola yang konsisten. Dalam berbagai kasus tersebut, penyalahgunaan *spyware* umumnya terjadi karena lemahnya *safeguard*, terutama dalam bentuk pengawasan oleh lembaga independen, mekanisme notifikasi kepada korban, dan transparansi.

Indonesia, dengan sejarah otoritarianisme Orde Baru dan kelemahan institusional hukum, menghadapi risiko yang jauh lebih besar. Oleh karena itu, *safeguard* yang dikembangkan untuk Indonesia harus lebih ketat daripada standar minimum internasional, dengan penekanan khusus pada pengawasan sipil independen, akuntabilitas, dan pemulihan bagi korban.

Salah satu kelemahan mendasar dalam kerangka hukum Indonesia saat ini adalah ketiadaan pembatasan yang jelas antara penggunaan *spyware* dalam konteks penegakan hukum (gakkum) dan pertahanan keamanan (hankam). Perbedaan ini bukan sekadar formalitas administratif, melainkan fundamental untuk mencegah penyalahgunaan dan memastikan akuntabilitas. Dalam konteks internasional, Dalam standar internasional untuk surveilans, dirangkum menjadi “*Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*”. Praktik surveilans semestinya tunduk pada elemen-elemen berikut: (i) *legality*; (ii) *legitimate aim*; (iii) *necessity*; (iv) *adequacy/proportionality*; (v) *competent judicial authority*; (vi) *due process*; (vii) *user notification*; dan (viii) *transparency*.⁴⁴

Dengan merujuk pada prinsip-prinsip internasional tersebut, Indonesia perlu menerjemahkannya ke dalam kerangka regulasi nasional yang lebih operasional dan ketat, terutama mengingat karakter *spyware* yang jauh lebih invasif serta lemahnya pembatasan kewenangan antar lembaga. Karena itu, rekomendasi kebijakan utama untuk Indonesia mencakup hal-hal berikut:

1. Definisi yang jelas tentang *spyware* dan perbedaannya dari penyadapan tradisional

Kerangka hukum Indonesia harus dimulai dengan definisi yang jelas tentang *spyware* dan teknologi surveilans invasif lainnya. Definisi ini harus mencakup karakteristik teknis yang

⁴³ Access Now et al., *International Principles on the Application of Human Rights to Communications Surveillance* (2014), <https://necessaryandproportionate.org/principles> (diakses pada 20 Januari 2026).

⁴⁴ *Ibid.*

membuat *spyware* jauh lebih invasif daripada alat penyadapan konvensional. Perbedaan ini penting karena *spyware* merepresentasikan tingkat intrusi yang secara kualitatif berbeda dibanding penyadapan menggunakan alat sadap tradisional. Sementara penyadapan tradisional terbatas pada komunikasi tertentu yang sedang berlangsung, *spyware* memberikan akses total ke seluruh kehidupan digital seseorang, termasuk data historis dan aktivitas yang tidak terkait dengan komunikasi. Hal ini sejalan dengan prinsip *legality*, yang mensyaratkan pembatasan HAM harus diatur dengan hukum yang jelas, presisi, dan dapat diperkirakan penerapannya. Tanpa definisi tegas, *spyware* akan beroperasi dalam wilayah abu-abu yang membuka ruang penyalahgunaan.

2. Pembatasan ketat pengguna *spyware*

Salah satu masalah paling krusial dalam konteks Indonesia adalah tumpang tindih kewenangan antara lembaga gakkum dan hankam dalam pengadaan dan penggunaan *spyware*. Hal ini sejalan dengan prinsip *legitimate aim dan necessity*, yang menegaskan bahwa surveilans hanya boleh dilakukan untuk tujuan sah yang benar-benar diperlukan dalam masyarakat demokratis, serta tidak boleh diperluas menjadi alat kontrol politik atau *discretionary power* aparat keamanan. Saat ini, Polri sebagai lembaga gakkum dapat merencanakan kebutuhan *spyware* yang kemudian masuk ke kategori hankam melalui pengadaan oleh Kementerian Pertahanan atau lembaga intelijen. Praktik ini menciptakan celah yang berbahaya karena:

- Menghindari pertanggungjawaban yudisial: Surveilans dalam konteks gakkum umumnya memerlukan surat perintah pengadilan, sementara surveilans hankam sering kali hanya memerlukan otorisasi internal atau presiden.
- Mengaburkan akuntabilitas: Ketika *spyware* yang digunakan untuk tujuan gakkum diperoleh melalui jalur hankam, menjadi tidak jelas lembaga mana yang bertanggung jawab atas penggunaannya.
- Memperluas ruang lingkup penggunaan: *Spyware* yang diperoleh untuk hankam dapat digunakan untuk tujuan yang lebih luas daripada yang diizinkan dalam konteks gakkum.

Sehingga pemisahan yang jelas penggunaan *spyware* untuk gakkum dan hankam dapat dilihat dalam tabel berikut:

Konteks	Gakkum	Hankam
Institusi	Lembaga penegakan hukum sipil (Polisi/Kejaksaan/PPNS) Penggunaan tunduk pada KUHP dengan surat perintah pengadilan	Lembaga intelijen (BIN atau TNI) untuk keamanan nasional tunduk pada UU intelijen
Pengadaan	Melalui proses tender terbuka dengan pengawasan Komisi III DPR dan BPK. Dialokasikan secara	Bagian dari rahasia negara, namun tetap dengan pengawasan dari Komisi I DPR

	eksplisit dalam APBN dan tidak boleh disamarkan dalam pos anggaran lain.	RI dan lembaga audit khusus. Dengan mekanisme informasi pengadaan dapat dibuka setelah masa tertentu (seperti diatur dalam RUU Rahasia Negara)
Penggunaan	Investigasi kejahatan (terorisme, transnasional, korupsi, TPPO, narkoba dalam skala besar, TPPU, dll). Harus didasari bukti kuat dan sudah pernah dilakukan metode investigatif namun gagal, untuk pelaksanaan harus dengan surat perintah pengadilan. Serta durasi sesuai yang diatur undang-undang.	Untuk ancaman nasional yang didefinisikan secara sempit (spionase asing, terorisme transnasional, ancaman terhadap infrastruktur kritis), harus ada asesmen bahwa target memang ancaman nyata untuk keamanan nasional. Durasi surveilans harus tetap dibatasi dan ditinjau ulang secara berkala.

1. Kewajiban notifikasi

Pemberitahuan harus diberikan kepada individu yang menjadi sasaran *spyware* setelah kegiatan pengawasan berakhir, kecuali apabila pemberitahuan tersebut dapat membahayakan investigasi yang masih berlangsung. Sebagaimana ditegaskan dalam perkara *Ekimdzhiiev v. Bulgaria*, notifikasi wajib dilakukan tanpa penundaan setelah jangka waktu yang benar-benar diperlukan untuk tujuan pengawasan yang sah telah terlampaui.

Pemberitahuan tersebut harus memuat informasi mengenai fakta bahwa individu pernah menjadi target pengawasan, lamanya pengawasan dilakukan, jenis data yang dikumpulkan, serta hak individu untuk menggugat keabsahan tindakan pengawasan tersebut. Setiap penundaan notifikasi harus dibatasi secara ketat dan hanya dapat dilakukan dengan persetujuan dari otoritas peradilan independen. Hal ini merupakan salah satu aspek penting untuk dimasukkan dalam pengaturan kedepannya, berakar langsung pada prinsip *User Notification dan Due Process*, karena tanpa kewajiban pemberitahuan, korban tidak memiliki akses terhadap pemulihan, dan surveilans akan beroperasi tanpa mekanisme kontrol demokratis yang efektif.

2. Mekanisme akuntabilitas

Tersedianya mekanisme yang memungkinkan korban surveilans untuk mendapatkan pemulihan jika *spyware* digunakan secara melanggar hukum. Ini termasuk:

- Penghapusan data yang dikumpulkan secara ilegal dari semua sistem pemerintah dan pemusnahan semua salinan.

- Pengakuan publik atas pelanggaran yang terjadi, termasuk permintaan maaf resmi dari negara.
- Sanksi administratif dan pidana terhadap pejabat yang menyalahgunakan *spyware*.
- Reformasi institusional untuk mencegah terulangnya pelanggaran serupa di masa depan.

3. Perlindungan khusus untuk kelompok berisiko tinggi

Termasuk di dalamnya jurnalis, pengacara, aktivis dan pembela HAM, politisi oposisi, serta kelompok lain yang memiliki peran penting dalam kehidupan demokratis. Penggunaan *spyware* terhadap kelompok-kelompok ini harus diatur dengan standar pengawasan yang jauh lebih ketat, dengan asumsi awal bahwa tindakan surveilans terhadap mereka pada dasarnya tidak sah, kecuali terdapat bukti yang sangat kuat bahwa mereka terlibat dalam tindak pidana berat. Selain itu, harus tersedia mekanisme khusus untuk menjamin perlindungan kerahasiaan sumber jurnalistik serta hak istimewa komunikasi antara pengacara dan klien.

4. Larangan pengadaan *spyware* dari vendor dengan rekam jejak pelanggaran HAM

Pemerintah harus melakukan uji tuntas HAM (*human rights due diligence*) sebelum membeli *spyware* dari vendor mana pun, termasuk investigasi tentang apakah vendor tersebut telah terlibat dalam penyediaan teknologi yang digunakan untuk melanggar HAM di negara lain. Vendor yang terbukti terlibat dalam pelanggaran HAM harus masuk dalam daftar hitam dan dilarang berbisnis dengan pemerintah Indonesia.

5. Pengawasan independen sebagai prasyarat implementasi

Indonesia saat ini tidak memiliki institusi dengan mandat dan kapasitas setara. Karena pembentukan lembaga baru akan sulit secara politik dan fiskal, opsi paling realistis adalah memperkuat mandat Komnas HAM melalui amandemen UU No. 39 Tahun 1999 dan regulasi turunan yang secara eksplisit memberikan kewenangan pengawasan surveilans digital. Penguatan ini harus mencakup akses terhadap informasi rahasia terkait *spyware*, kapasitas audit forensik digital, koordinasi dengan DPR, BPK, dan pengadilan, serta mekanisme rekomendasi yang dapat dipaksakan dalam kasus pelanggaran HAM serius. Langkah ini sejalan dengan Paris Principles yang menegaskan bahwa lembaga HAM nasional harus memiliki mandat luas untuk mengawasi seluruh isu HAM, termasuk pelanggaran yang muncul dari teknologi baru seperti surveilans. Dengan mandat yang diperkuat, Komnas HAM dapat berfungsi secara preventif dan represif: memantau penggunaan *spyware* oleh aparat negara, memanggil lembaga pengguna maupun vendor, memastikan adanya *human rights due diligence* sesuai UN Guiding Principles on

Business and Human Rights, serta mengeluarkan rekomendasi publik dan mekanisme pemulihan apabila ditemukan penyalahgunaan yang melanggar hak asasi manusia.

Apabila ditemukan indikasi serius penyalahgunaan yang melanggar hak asasi manusia, Komnas HAM berwenang mengeluarkan rekomendasi publik, menyatakan praktik tersebut melanggar HAM dan harus dihentikan, serta menyediakan mekanisme perlindungan dan pemulihan bagi korban penyalahgunaan teknologi surveilans.

Fungsi Komnas HAM dalam konteks ini dapat dibagi menjadi dua kategori utama: preventif (mencegah penyalahgunaan sebelum terjadi) dan represif (merespons penyalahgunaan yang sudah terjadi). Pembagian ini mencerminkan pendekatan holistik terhadap pengawasan yang tidak hanya reaktif terhadap pelanggaran, tetapi juga proaktif dalam mencegahnya.

Preventif	Represif
Memberikan capacity building mengenai 13 prinsip surveilans	Penyelidikan atas aduan atau inisiatif lembaga
Menyusun <i>surveillance guideline</i> berisi hal principal tanpa detail teknis yang dapat diakses publik sebagai materi pendidikan publik	Mendorong pengakuan negara jika terindikasi surveilans melanggar ham
Melakukan asesmen dalam pengadaan <i>spyware</i>	mengeluarkan rekomendasi publik, menyatakan praktik tersebut melanggar HAM dan harus dihentikan
Monitoring investigasi internasional tentang vendor <i>spyware</i> , melakukan evaluasi berkala vendor yang sudah digunakan pemerintah Indonesia serta Menyusun rekomendasi pemberhentian kontrak dan daftar hitam vendor dengan rekam jejak pelanggaran HAM seperti pegasus	menyediakan mekanisme perlindungan dan pemulihan bagi korban penyalahgunaan teknologi surveilans.

Kompleksitas Industri Militer

Pergeseran menuju *surveillance-based security* terjadi dalam ekosistem industri pertahanan yang kompleks, tertutup, dan minim akuntabilitas. Penelusuran dokumen anggaran negara periode 2018-2024 ditemukan hampir 36 triliun dialokasikan untuk pengadaan teknologi surveilans di empat institusi utama (Kejaksaan RI, Kementerian Pertahanan, Badan Siber dan Sandi Negara).⁴⁵ Angka ini kemungkinan yang terdeteksi,

⁴⁵ Lihat Kezia Khatwani dkk., *Privasi dalam Rumah Kaca: Menuntut Akuntabilitas Penggunaan Spyware di Indonesia* (Jakarta: ELSAM, 2026), hlm 279.

mengingat banyak pos anggaran yang tidak terpublikasi atau dilabeli dengan nama-nama teknis hingga menyulitkan penelusuran.

Pengadaan teknologi surveilans memiliki pola yang konsisten dan bermasalah. Pertama, ketidaktransparanan sistemik. Data pengadaan sangat sulit ditelusuri, banyak item anggaran dilabeli sebagai aset negara yang secara otomatis menutup akses publik.

Dalam konteks UU Pertahanan Negara dan UU Keterbukaan Informasi Publik (KIP), memang ada ruang pengecualian untuk urusan-urusan yang dapat dikecualikan dari publikasi. Namun, pengecualian ini telah digunakan secara luas hingga menciptakan anggaran yang hampir tidak dapat diaudit publik. Dokumen anggaran yang tersedia berdasarkan penelusuran, sering menggunakan nomenklatur teknis yang mengaburkan substansi pengadaan misalnya “peralatan komunikasi khusus,” “sistem informasi terintegrasi,” atau bahkan kode-kode internal seperti “James Bond Kit” sehingga sulit untuk memahami apa yang sebenarnya dibeli dan untuk tujuan apa.

Dominasi Penunjukan Langsung dalam Pengadaan Sistem Pertahanan

Dominasi penunjukan langsung dalam pengadaan teknologi surveilans di Indonesia berakar pada pemanfaatan celah legalitas dalam UU Pertahanan Negara dan UU KIP yang memberikan ruang pengecualian atas dasar rahasia negara. Hal ini kemudian diperkuat sebagaimana dijelaskan dalam Peraturan Menteri Pertahanan Nomor 16 Tahun 2019 yang telah diubah melalui Peraturan Menteri Pertahanan Nomor 14 Tahun 2020 tentang Pelaksanaan Pengadaan Alat Peralatan Pertahanan dan Keamanan di Lingkungan Kementerian Pertahanan dan tentara Negara Indonesia yang merupakan turunan dari Peraturan Presiden Nomor 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah. Mekanisme ini sering kali menjadi jalur utama bagi institusi seperti Kemenhan, Kejaksaan, hingga BSSN untuk menghindari proses lelang kompetitif dengan dalih menjaga kerahasiaan spesifikasi teknis dan urgensi keamanan nasional.

Secara ekosistem, pola ini menciptakan ketergantungan kronis pada segelintir vendor “langganan” yang dikontrak dalam jangka Panjang. Praktik ini menyebabkan adanya risiko *lock-in* yang mana menjadi salah satu kelemahan terbesar sebagai risiko terjebak pada penyedia yang tidak lagi kompetitif atau ketika kondisi pasar berubah. *Lock-in* dapat menyebabkan biaya tinggi, penurunan kualitas, atau ketidakmampuan beradaptasi terhadap inovasi baru.⁴⁶ Hal ini juga menimbulkan akses khusus ke lingkaran pengambil kebijakan. Akibatnya, penunjukan langsung bukan lagi menjadi pengecualian yang dilakukan dalam kondisi darurat, melainkan telah bergeser menjadi norma pengadaan yang melanggengkan struktur pasar oligopolistic dan menutup pintu inovasi bagi penyedia teknologi lainnya.

⁴⁶ LSP Pengadaan Indonesia, “Kontrak Jangka Pendek vs Jangka Panjang”, *LSP Pengadaan Indonesia*, 2023, <https://lsp Pengadaan.id/kontrak-jangka-pendek-vs-jangka-panjang/> (diakses pada 20 Januari 2026)

Penunjukkan langsung yang didasarkan pada beberapa ketentuan sebagaimana dijelaskan dalam Peraturan Presiden Nomor 27 Tahun 2019 tentang Syarat dan Tata Cara Pengadaan Peralatan Pertahanan dan Keamanan Produk Industri Pertahanan dengan Kontrak Jangka Panjang melalui penugasan pemerintah (“penunjukan langsung”) dapat berisiko terhadap adanya *lock-in* tersebut.⁴⁷

Di sisi lain, dominasi metode penunjukan langsung ini berdampak pada kaburnya akuntabilitas anggaran yang mencapai triliunan rupiah. Penggunaan nomenklatur teknis yang samar seperti “peralatan komunikasi khusus” atau kode internal yang tidak lazim berfungsi sebagai tameng tambahan untuk menyembunyikan substansi pengadaan dari audit publik dan pengawasan masyarakat sipil.

Tanpa adanya perbandingan harga pasar yang dihasilkan dari proses lelang terbuka, risiko terjadinya penggelembungan biaya (*mark-up*) menjadi sangat tinggi dan sulit dideteksi. Hal ini memperparah ketidaktransparanan sistemik dalam industri pertahanan, di mana pengalokasian dana besar untuk teknologi surveilans seolah-olah masuk ke dalam “kotak hitam” yang hanya bisa diakses oleh aktor-aktor tertentu sehingga esensi dari efektivitas belanja negara demi keamanan rakyat seringkali terabaikan oleh konflik kepentingan.

Maka dari hal ini diperlukan adanya pengawasan yang ketat dalam pelaksanaannya dengan solusi hybrid dengan mekanisme *performance-based long-term contract* yang menekankan pada *Key-Performance-Indicator* (KPI), audit berkala, dan mekanisme negosiasi untuk mengatasi perubahan.

Rantai Pasok yang Kabur, Biaya yang Tinggi, dan Tidak Transparan

Rantai pasok dalam pengadaan sistem pertahanan dan teknologi surveilans sering kali sengaja dirancang secara berlapis guna menyamarkan asal-usul teknologi serta aktor di balik transaksi tersebut. Penggunaan Perusahaan cangkang (*shell companies*) atau perantara pihak ketiga (*middlemen*) menjadi praktik umum yang mengaburkan jejak manufaktur asli, terutama ketika perangkat tersebut berasal dari negara dengan reputasi hak asasi manusia yang kontroversial atau vendor yang masuk dalam daftar hitam internasional. Struktur yang kabur ini tidak hanya mempersulit pelacakan aliran dana negara, tetapi juga menciptakan celah bagi praktik lobi terselubung di mana keuntungan ekonomi terkonsentrasi pada jejaring elit yang menghubungkan birokrasi militer dengan broker swasta tanpa adanya audit rantai pasok yang memadai.

Ketidakjelasan rantai pasok ini berdampak fatal pada kedaulatan digital dan keamanan nasional karena perangkat yang dibeli melalui jalur tidak transparan berisiko membawa

⁴⁷ Amanda Kusumawardhani, “Pengadaan Alat Pertahanan dan Keamanan Lewat Kontrak Jangka Panjang, Ini Aturannya”, *Kabar 24*, 8 Mei 2019, https://kabar24.bisnis.com/read/20190508/15/919963/pengadaan-alat-pertahanan-dan-keamanan-lewat-kontrak-jangka-panjang-ini-aturannya#goog_rewarded (diakses pada 20 Januari 2026).

celah keamanan (*backdoors*) yang tidak terdeteksi. Tanpa adanya kewajiban bagi vendor untuk membuka transparansi komponen atau asal-usul perangkat tersebut, negara sebenarnya sedang membeli “kotak hitam” yang fungsionalitasnya bisa saja dikendalikan oleh pihak asing. Minimnya akuntabilitas dalam rantai pasok ini mempertegas bahwa pengadaan teknologi surveilans bukan sekadar masalah teknis pertahanan, melainkan refleksi dari ekosistem industri yang sangat tertutup, di mana kepentingan keamanan publik sering kali dikalahkan oleh kerahasiaan operasional yang melindungi keuntungan ekonomi para pemain kunci di dalamnya.

Contoh riilnya seperti pada pengadaan teknologi alutsista dan non-alutsista termasuk *spyware*. Jika dikaitkan dengan analisis anggaran fungsi pertahanan pada tahun 2023, anggaran fungsi pertahanan turun 3,7 persen dari tahun 2022 menjadi Rp144.685,6 miliar pada tahun 2023. Anggaran fungsi pertahanan tahun 2023 akan digunakan untuk pengadaan dan pemeliharaan alutsista dan non-alutsista, penguatan pertahanan di wilayah perbatasan, penegakan kedaulatan di daerah perairan Indonesia, dan bela negara, antara lain karena efisiensi pengelolaan organisasi dan sumber daya manusia Kemenhan.⁴⁸

Anggaran pertahanan yang mencapai ratusan triliun rupiah dengan rantai pasok yang kabur menimbulkan celah risiko inefisiensi dan akuntabilitas. Ketika anggaran fungsi pertahanan tahun 2023 sebesar Rp144,6 triliun digunakan untuk pengadaan yang tidak terbatas pada senjata utama, tetapi juga “peralatan non-alutsista” dan “penguatan pertahanan perbatasan”, nomenklatur yang digunakan sering kali menjadi sangat umum dan multitafsir. Dalam ekosistem yang tertutup, istilah-istilah *generic* ini sering kali menjadi pintu masuk bagi teknologi surveilans termasuk *spyware* atau perangkat intelijen yang pengadaanya dilakukan melalui vendor perantara. Rantai pasok yang tidak transparan menyebabkan publik tidak dapat memastikan apakah kontraksi anggaran 3,7% tersebut benar-benar merupakan hasil efisiensi atau justru merupakan pengalihan dana ke pos-pos pengadaan yang sulit diaudit karena identitas manufaktur aslinya disembunyikan di balik Perusahaan cangkang.

Lebih jauh lagi, penggunaan anggaran untuk “pemeliharaan” dan “pemenuhan” dalam sistem yang rantai pasoknya kabur menciptakan ketergantungan jangka panjang terhadap penyedia pihak ketiga yang identitasnya tidak terekspos. Aliran dana dari total pagu Rp144,6 triliun tersebut berisiko terjebak dalam skema *middlemen* yang mengambil margin keuntungan besar, terutama untuk komponen teknologi sensitif yang diklaim sebagai pendukung kedaulatan di wilayah perbatasan. Tanpa adanya transparansi rantai pasok, klaim mengenai “efisiensi pengelolaan organisasi” menjadi sulit diverifikasi, karena publik tidak memiliki akses untuk mengetahui apakah harga yang dibayar negara

⁴⁸ Kementerian Keuangan Republik Indonesia, *Buku II Nota Keuangan Beserta Rancangan Anggaran Pendapatan dan Belanja Negara Tahun 2024*, Kemenkeu, 2024.

sesuai dengan nilai barang di pasar internasional atau telah terbebani oleh biaya lobi dan perantara. Pada akhirnya, besarnya angka anggaran yang dialokasikan justru mempertegas urgensi pengawasan rantai pasok agar dana pertahanan tidak hanya habis untuk memperkaya aktor-aktor di jalur pengadaan yang gelap, melainkan benar-benar untuk penguatan kedaulatan negara.

Implementasi UU Keterbukaan Informasi Publik (KIP) dalam ekosistem industri militer sering kali terbentur oleh dinding tebal "rahasia negara" yang digunakan secara ekstensif untuk menutupi jejak pengadaan teknologi surveilans. Meskipun UU KIP secara filosofis menjamin hak publik atas transparansi anggaran, Pasal 17 dalam undang-undang tersebut memberikan ruang pengecualian yang luas bagi informasi yang dianggap dapat membahayakan pertahanan dan keamanan nasional. Celah inilah yang sering kali dieksploitasi untuk menyembunyikan identitas vendor perantara atau perusahaan cangkang di balik nomenklatur teknis yang kabur. Akibatnya, proses uji konsekuensi yang seharusnya dilakukan secara ketat oleh pejabat publik sering kali hanya menjadi formalitas untuk menolak permohonan informasi terkait aliran dana triliunan rupiah yang mengalir ke pihak ketiga yang tidak jelas asal-usulnya.

Kelemahan sistemik ini diperparah oleh fakta bahwa regulasi kita saat ini belum mewajibkan pengungkapan pemilik manfaat (*beneficial ownership*) secara transparan dalam setiap kontrak pengadaan strategis. Ketika sebuah instansi pemerintah menunjuk vendor perantara melalui mekanisme penunjukan langsung, kewajiban pelaporan sering kali berhenti pada entitas legal di permukaan, tanpa menelusuri siapa manufaktur asli atau aktor intelektual di belakangnya. Hal ini menciptakan anomali hukum di mana dana publik digunakan untuk membeli teknologi sensitif, namun publik kehilangan haknya untuk mengetahui apakah vendor tersebut memiliki rekam jejak pelanggaran HAM atau potensi kebocoran data ke pihak asing. Tanpa adanya sinkronisasi antara UU KIP dan pengawasan ketat terhadap rantai pasok industri pertahanan, transparansi pengadaan akan terus menjadi korban dari narasi keamanan yang tertutup dan minim akuntabilitas.

Oleh karena itu, pemerintah perlu membangun tata kelola pengadaan teknologi pertahanan yang tetap menjunjung prinsip transparansi dan akuntabilitas. Meskipun informasi tertentu dapat dikecualikan demi kepentingan keamanan nasional, pengecualian tersebut tidak boleh menutup seluruh proses pengadaan dari pengawasan publik.

Sekuritisasi dan Narasi Keamanan Nasional dalam Pengadaan Sistem Pertahanan

Sekuritisasi merupakan proses pengidentifikasian isu-isu lingkungan, sosial, politik, ekonomi menjadi isu keamanan bagi negara.⁴⁹ Dalam konteks industri militer, sekuritisasi

⁴⁹ Yusa Djuyandi, Hasya Aiman Nadhir, Afifah Amaliya Pohan, Duta Smaradana, Adisa Naura Priadi, Proses Sekuritisasi dan Desekuritisasi dalam Upaya Menurunkan Angka Kasus Covid-19 di Indonesia, *Jurnal Wacana Publik*, Volume 16, Nomor 1, 2023, halaman. 1-12.

adalah proses politik di mana suatu isu seperti teknologi informasi atau pengadaan barang diangkat dari ranah politik biasa menjadi masalah keamanan eksistensial yang mendesak. Melalui narasi keamanan nasional yang kuat, aktor-aktor negara dapat membenarkan penggunaan langkah-langkah luas biasa termasuk pengabaian prosedur lelang standar dan penggunaan mekanisme penunjukan langsung. Narasi ini menciptakan pembenaran moral dan legal bahwa transparansi harus dikalahkan demi kerahasiaan operasional sehingga anggaran sebesar Rp144,6 triliun atau pengadaan teknologi surveilans termasuk *spyware* dapat diproses di luar jangkauan pengawasan publik. Sekuritisasi mengubah alutsista dan perangkat surveilans termasuk *spyware* bukan sebagai instrumen teknis, melainkan sebagai simbol kedaulatan yang tidak boleh dipertanyakan efektivitas biaya atau rantai pasoknya.

Dampak dari narasi keamanan nasional ini adalah terbentuknya “ruang gelap” dalam penganggaran yang membatasi akuntabilitas publik dan lembaga audit. Ketika sebuah pengadaan dilabeli sebagai instrumen vital untuk “pertahanan dan keamanan”, kritik terhadap inefisiensi atau kaburnya rantai pasok sering kali dituduh sebagai upaya melemahkan ketahanan negara.

Narasi ini secara efektif membungkam perdebatan mengenai apakah penggunaan perusahaan cangkang atau perantara pihak ketiga merupakan risiko keamanan siber dan pemborosan anggaran. Akhirnya, sekuritisasi berfungsi sebagai instrumen untuk melanggengkan ekosistem industri militer yang tertutup, di mana kepentingan elit ekonomi dan birokrasi berlindung di balik jargon keamanan nasional untuk menghindari audit dan transparansi yang seharusnya melekat pada setiap penggunaan dana negara.

Lemahnya Mekanisme Pengawasan

Lemahnya mekanisme *check and balances* dalam pengadaan sistem pertahanan di Indonesia berakar pada dominasi otoritas eksekutif yang sering kali tidak diimbangi oleh pengawasan legislatif maupun audit independen yang mendalam. Dalam ekosistem yang tertutup ini, DPR sering kali hanya melakukan pengawasan pada level pagu anggaran tanpa mampu menelaah rincian teknis pengadaan teknologi seperti *spyware* karena alasan kerahasiaan negara. Pada saat yang sama, Badan Pemeriksa Keuangan (BPK) juga menghadapi keterbatasan akses untuk memverifikasi kewajaran harga dan asal-usul rantai pasok. Kondisi ini melemahkan mekanisme pengawasan dan akuntabilitas dalam pengadaan teknologi pertahanan.

Persoalan lain yang turut meningkatkan risiko penyimpangan adalah penggunaan metode penunjukan langsung dalam pengadaan alat pertahanan. Meskipun metode ini dapat dibenarkan dalam kondisi tertentu, minimnya kompetisi dan transparansi menjadikannya lebih rentan terhadap praktik korupsi maupun konflik kepentingan apabila tidak disertai mekanisme pengawasan yang memadai.

Kasus nyata yang menggambarkan kerentanan ini adalah laporan investigasi mengenai masuknya *spyware* tingkat tinggi seperti Pegasus ke Indonesia yang sering kali tidak tercatat secara eksplisit dalam dokumen publik pengadaan alutsista. Pegasus merupakan alat penyadap milik Perusahaan NSO Group asal Israel yang dilaporkan telah dimiliki oleh sejumlah lembaga intelijen dan penegak hukum di Indonesia.⁵⁰ Pengadaan teknologi ini kerap menggunakan Perusahaan perantara (vendor pihak ketiga) untuk mengaburkan manufaktur aslinya, sehingga sulit bagi publik maupun lembaga pengawas untuk memastikan apakah teknologi ini dibeli untuk kepentingan pertahanan negara atau justru untuk memata-matai warga sipil. Lemahnya pengawasan ini menjadi bukti nyata bahwa militerisasi teknologi digital di Indonesia sedang berlangsung dalam ruang hampa akuntabilitas yang sangat membahayakan demokrasi.

Gagasan Perlindungan Hukum dan HAM dalam Lanskap Digital

Reformasi pengaturan pengadaan teknologi militer menjadi kebutuhan yang mendesak. Salah satu langkah yang perlu dilakukan adalah mengintegrasikan standar hak asasi manusia ke dalam proses pemilihan vendor. Dalam konteks militerisasi teknologi, pengadaan *spyware* tidak boleh lagi diposisikan sebagai belanja rutin “peralatan khusus”, melainkan harus melalui proses audit ketat untuk memastikan perangkat tersebut tidak digunakan untuk menyerang privasi warga secara semena-mena. Tanpa transparansi dalam pengadaan dan pengaturan yang ketat mengenai penggunaannya, teknologi pertahanan dapat dengan mudah disalahgunakan untuk melanggar hak asasi manusia.

Mekanisme pengawasan yudisial, seperti kewajiban memperoleh izin pengadilan sebelum penyadapan dan tersedianya mekanisme praperadilan, merupakan instrumen penting untuk mencegah penyalahgunaan teknologi pengawasan terhadap warga sipil. Hal ini sebagaimana dijelaskan dalam Pasal 30 dan Pasal 31 ayat (1) dan (2) UU ITE, Pasal 258 dan Pasal 332 Kitab Undang-Undang Hukum Pidana, Pasal 40 UU Telekomunikasi, Pasal 65 jo. Pasal 67 UU PDP, dan RUU Penyadapan yang pada intinya melarang setiap orang melakukan penyadapan terhadap informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun. Kata “setiap orang” dalam hal ini tidak terkecuali bagi aparat pemerintah dan penegak hukum apalagi digunakan untuk memata-matai.

Penggunaan perangkat penyadapan atau intersepsi komunikasi di ranah domestik harus didasarkan pada perintah pengadilan (*judicial warrant*) yang independen, bukan semata-mata atas dasar diskresi pimpinan lembaga keamanan. Mekanisme ini penting untuk memastikan bahwa teknologi tersebut hanya digunakan untuk tujuan yang sah dan tidak

⁵⁰ Tibiko Zabari, “Waspada Ancaman Demokrasi: Awasi Penggunaan, Polri Harus Buka Informasi Pengadaan “Kuda Terbang””, *Aliansi Jurnalis Independen*, 2023, <https://aji.or.id/informasi/waspada-ancaman-demokrasi-awasi-penggunaan-polri-harus-buka-informasi-pengadaan-kuda> (diakses pada 20 Januari 2025)

disalahgunakan untuk memantau kritik atau aktivitas masyarakat yang dilindungi oleh hak asasi manusia.

Reformasi sektor keamanan harus diarahkan pada penataan kewenangan penggunaan teknologi surveilans, khususnya *spyware*, agar tetap sesuai dengan mandat masing-masing lembaga. Reformasi ini memerlukan pembagian peran yang tegas antara intelijen militer, intelijen kepolisian, dan badan siber untuk mencegah tumpang tindih kewenangan maupun penyalahgunaan *spyware*. Melalui reformasi tersebut, penggunaan teknologi surveilans diharapkan lebih akuntabel dan terbuka terhadap pengawasan sipil yang efektif, sehingga tidak disalahgunakan untuk kepentingan politik praktis atau pengawasan yang sewenang-wenang terhadap masyarakat sipil.

Mekanisme pemulihan (*remedy*) yang efektif harus tersedia bagi individu yang menjadi korban penggunaan *spyware*. Mengingat sifat *spyware* yang sangat invasif, negara wajib menyediakan jalur hukum di mana korban dapat menuntut pertanggungjawaban dan mendapatkan rehabilitasi jika hak privasinya dilanggar tanpa dasar hukum yang sah. Mekanisme ini berfungsi sebagai kontrol sosial yang memastikan bahwa setiap aktor keamanan yang menyalahgunakan teknologi militer akan menghadapi konsekuensi hukum yang setimpal, sekaligus memberikan keadilan bagi masyarakat terdampak.

Penggunaan *spyware* tanpa kontrol hak asasi manusia yang memadai berpotensi menciptakan iklim ketakutan yang merusak kualitas demokrasi di Indonesia. Penggunaan *spyware* dalam operasi keamanan yang tidak transparan juga menimbulkan ketidakpastian hukum karena mengaburkan batas antara upaya menjaga keamanan nasional dan tindakan represif terhadap aktivis, jurnalis, maupun masyarakat sipil. Apabila tidak segera diatur melalui kerangka hukum yang memadai, *spyware* yang semestinya digunakan untuk kepentingan pertahanan dan keamanan justru berpotensi menjadi instrumen yang membatasi kebebasan sipil dan melemahkan prinsip-prinsip demokrasi.

Penguatan akuntabilitas hukum dan penghormatan terhadap hak asasi manusia dalam pengadaan dan penggunaan teknologi pertahanan bukan sekadar persoalan teknis, melainkan komitmen untuk memastikan bahwa kebijakan keamanan nasional tetap sejalan dengan prinsip negara hukum dan hak asasi manusia. Indonesia perlu memastikan bahwa setiap rupiah yang dialokasikan untuk teknologi pertahanan digital tidak hanya memperkuat otot militer, tetapi juga melindungi hak-hak dasar warga negara. Integrasi mekanisme pengawasan yudisial, reformasi sektor keamanan, dan sistem pemulihan yang kuat adalah harga mati agar militerisasi teknologi tidak berubah menjadi tirani digital yang tidak tersentuh hukum.

PENUTUP

Kesimpulan

Uraian mengenai militerisasi teknologi, khususnya terkait pengadaan dan penggunaan *spyware*, dan implikasinya terhadap hak asasi manusia di atas dapat disimpulkan sebagai berikut:

1. Indonesia tengah mengalami pergeseran paradigma keamanan dari pertahanan tradisional menjadi *surveillance-based security* yang sangat bergantung pada kemampuan memantau dan menganalisis data secara masif. Hal ini didorong oleh peningkatan anggaran pertahanan serta agresivitas pemerintah dalam menjalin kerja sama teknologi militer dengan mitra internasional.
2. Terdapat kesenjangan fundamental antara kemajuan teknologi *spyware* modern yang memiliki kemampuan *zero-click* dengan regulasi hukum di Indonesia yang masih tertinggal dan hanya mengatur penyadapan tradisional. Kondisi ini menciptakan kekosongan hukum yang berbahaya karena teknologi digital saat ini mampu mengonversi perangkat pribadi menjadi alat pengawasan permanen tanpa batas ruang dan waktu.
3. Pengadaan teknologi surveilans di Indonesia beroperasi dalam ekosistem tertutup dan minim akuntabilitas, di mana narasi “keamanan nasional” sering digunakan untuk menghindari proses audit publik dan mekanisme lelang kompetitif. Dominasi penunjukan langsung dan penggunaan perusahaan perantara mengaburkan rantai pasok asli, sehingga meningkatkan risiko inefisiensi anggaran serta potensi ketergantungan pada vendor dengan rekam jejak HAM yang buruk.
4. Penggunaan *spyware* tanpa pengawasan yudisial yang independen berpotensi menciptakan zona bebas hukum yang mengancam kebebasan berekspresi, privasi, dan partisipasi politik. Militerisasi teknologi digital tanpa kontrol yang memadai berisiko mengubah instrumen pertahanan menjadi alat represi terhadap jurnalis, aktivis, dan oposisi politik yang pada akhirnya dapat melemahkan sendi-sendi demokrasi dari dalam.
5. Untuk mencegah tirani digital, diperlukan reformasi sektor keamanan yang mengintegrasikan standar HAM sebagai syarat mutlak dalam pengadaan teknologi. Langkah krusial yang harus diambil mencakup penerapan izin pengadilan (*judicial warrant*), kewajiban notifikasi kepada target, serta penguatan mandat lembaga independen seperti Komnas HAM sebagai prasyarat pengawasan digital.

Rekomendasi

Untuk memperkuat tata kelola pengadaan dan penggunaan *spyware* serta mencegah penyalahgunaannya, pemerintah perlu mengambil langkah-langkah kebijakan sebagai berikut.

1. Menyusun pengaturan yang secara jelas mendefinisikan *spyware*, ruang lingkup penggunaannya, kewenangan lembaga yang dapat menggunakannya, serta syarat dan batasan penggunaannya sesuai dengan standar hak asasi manusia.
2. Menetapkan pembagian kewenangan yang jelas antara lembaga penegak hukum dan lembaga pertahanan-keamanan dalam pengadaan dan penggunaan *spyware* untuk mencegah tumpang tindih kewenangan serta memastikan setiap penggunaan *spyware* tunduk pada mekanisme pengawasan yang sesuai.
3. Mewajibkan pelaksanaan *human rights due diligence* sebelum pengadaan *spyware* serta melarang pengadaan dari vendor yang terbukti memiliki rekam jejak pelanggaran hak asasi manusia melalui mekanisme daftar hitam (*blacklisting*).
4. Menerapkan mekanisme otorisasi yudisial (*judicial warrant*) yang mewajibkan penggunaan perangkat penyadapan atau intersepsi komunikasi di ranah domestik memperoleh izin terlebih dahulu dari pengadilan yang independen. Penggunaan kewenangan tersebut tidak boleh semata-mata didasarkan pada diskresi pimpinan lembaga keamanan. Mekanisme ini penting untuk memastikan adanya batas yang jelas antara penggunaan teknologi surveilans dalam menghadapi ancaman terhadap keamanan nasional dan penggunaannya untuk memantau aktivitas masyarakat yang dilindungi oleh hak asasi manusia, termasuk kebebasan berekspresi dan kebebasan pers.
5. Mewajibkan lembaga yang berwenang melakukan surveilans untuk memberikan notifikasi kepada setiap individu yang menjadi sasaran surveilans. Pemberitahuan diberikan setelah kegiatan surveilans berakhir dan tidak lagi berpotensi mengganggu proses penegakan hukum atau kepentingan keamanan nasional yang sah. Kewajiban notifikasi ini penting untuk memastikan bahwa setiap individu memiliki kesempatan mengetahui tindakan yang dilakukan terhadapnya serta memperoleh akses terhadap upaya pemulihan (*remedy*) apabila hak-haknya dilanggar. Tanpa mekanisme tersebut, praktik surveilans berisiko berlangsung tanpa akuntabilitas dan pengawasan yang efektif.
6. Membentuk peraturan perundang-undangan yang mengatur penggunaan *spyware* dengan memberikan perlindungan yang lebih kuat bagi kelompok yang memiliki peran penting dalam kehidupan demokrasi, seperti jurnalis, pengacara, pembela hak asasi manusia, dan oposisi politik. Penggunaan *spyware* terhadap kelompok-kelompok tersebut hanya dapat dilakukan dalam keadaan yang sangat terbatas, berdasarkan bukti yang kuat mengenai keterlibatan dalam tindak pidana berat, serta harus memperoleh otorisasi yudisial. Regulasi tersebut juga harus menjamin kerahasiaan sumber jurnalistik dan kerahasiaan komunikasi antara pengacara dan klien.
7. Memperkuat pengawasan independen oleh Komnas HAM terhadap penggunaan *spyware* dan surveilans digital, penguatan kapasitas audit forensik, dan penguatan tindak lanjut atas rekomendasi Komnas HAM. Komnas HAM perlu menjalankan fungsi

preventif melalui asesmen terhadap pengadaan *spyware* serta fungsi represif melalui penyelidikan atas dugaan pelanggaran hak asasi manusia. Apabila ditemukan pelanggaran, Komnas HAM perlu mendorong negara untuk mengakui pelanggaran tersebut dan menindaklanjutinya melalui langkah-langkah pemulihan yang efektif bagi korban.

8. Mengatur mekanisme pemulihan (*remedy*) yang efektif bagi korban penyalahgunaan *spyware*, termasuk hak untuk mengajukan tuntutan, memperoleh rehabilitasi, dan meminta penghapusan data yang diperoleh secara melawan hukum. Mekanisme tersebut juga harus mencakup sanksi administratif dan pidana terhadap pejabat yang menyalahgunakan kewenangannya, serta reformasi kelembagaan untuk mencegah terulangnya pelanggaran serupa.

DAFTAR PUSTAKA

Access Now et al., "International Principles on the Application of Human Rights to Communications Surveillance", 2014, <https://necessaryandproportionate.org/principles> (diakses pada 20 Januari 2026).

Amanda Kusumawardhani, "Pengadaan Alat Pertahanan dan Keamanan Lewat Kontrak Jangka Panjang, Ini Aturannya", *Kabar 24*, 8 Mei 2019, https://kabar24.bisnis.com/read/20190508/15/919963/pengadaan-alat-pertahanan-dan-keamanan-lewat-kontrak-jangka-panjang-ini-aturannya#goog_rewarded (diakses pada 20 Januari 2026).

American Civil Liberties Union (ACLU), "Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress," *ACLU.org*, 11 April 2023, <https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress> (diakses pada 20 Januari 2026).

Amnesty International UK, "UK Government GCHQ Mass Spying Surveillance," *Amnesty.org.uk*, 1 April 2025, <https://www.amnesty.org.uk/knowledge-hub/all-resources/uk-government-gchq-ipt-mass-spying-surveillance/> (diakses pada 20 Januari 2026).

Antara News, "Menhan Bahas Kerja Sama Pertukaran Teknologi Militer dengan Jepang," *Antara News*, 7 Januari 2025, <https://www.antaranews.com/berita/4568354/menhan-bahas-kerja-sama-pertukaran-teknologi-militer-dengan-jepang> (diakses pada 20 Januari 2026).

BBC News Indonesia, "Demonstrasi mahasiswa menentang UU TNI berlangsung maraton dan menyebar ke banyak kota, apa maknanya?," *BBC News Indonesia*, 31 Maret 2025, <https://www.bbc.com/indonesia/articles/c0jgj0e4284o> (diakses pada 20 Januari 2026).

Brennan Center for Justice, "Privacy and Civil Liberties Oversight Board Embraces Surveillance Reforms," *BrennanCenter.org*, 11 Oktober 2023, <https://www.brennancenter.org/our-work/analysis-opinion/privacy-and-civil-liberties-oversight-board-embraces-surveillance-reforms> (diakses pada 20 Januari 2026).

Deutsche Welle (DW), "Greece Spy Chief Quits Amid Predator Spyware Furor," *DW*, 5 Agustus 2022, <https://www.dw.com/en/greece-spy-chief-quits-amid-predator-spyware-furor/a-62723640> (diakses pada 20 Januari 2026).

Deutsche Welle (DW), “Poland Top Leader Admits Government Bought Pegasus Spyware,” *DW*, 27 Desember 2021, <https://www.dw.com/en/poland-top-leader-admits-government-bought-pegasus-spyware/a-60361211> (diakses pada 20 Januari 2026).

European Court of Human Rights (Chamber), *Weber v. Switzerland* (Application no. 11034/84), *Judgment*, 22 Mei 1990, <https://hudoc.echr.coe.int/eng?i=001-57629> (diakses pada 20 Januari 2026).

European Court of Human Rights (Fifth Section), *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (Application no. 62540/00), *Judgment*, 28 Juni 2007, <https://hudoc.echr.coe.int/eng?i=001-81323> (diakses pada 20 Januari 2026).

European Court of Human Rights (Fourth Section), *Liberty and Others v. the United Kingdom* (Application no. 58243/00), *Judgment*, 1 Juli 2008, <https://hudoc.echr.coe.int/eng?i=001-87207> (diakses pada 20 Januari 2026).

European Court of Human Rights (Grand Chamber), *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14, and 24960/15), *Judgment*, 25 Mei 2021, <https://hudoc.echr.coe.int/fre?i=001-210077> (diakses pada 20 Januari 2026).

European Court of Human Rights (Grand Chamber), *Roman Zakharov v. Russia* (Application no. 47143/06), *Judgment*, 4 Desember 2015, <https://hudoc.echr.coe.int/fre?i=001-159324> (diakses pada 20 Januari 2026).

European Data Protection Board, Guidelines 10/2020 on Restrictions under Article 23 GDPR, version 2.0 (Brussels: EDPB, Oktober 2021), paras. 37–40.

European Parliament, “Parliament Establishes Inquiry Committee,” *European Parliament Committees*, 16 August 2022, <https://www.europarl.europa.eu/committees/en/parliament-establishes-inquiry-committee/product-details/20220816CHE10529> (diakses pada 20 Januari 2026).

European Parliament, Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware* (2022/2077(INI)), Rapporteur Sophie in 't Veld, 22 May 2023 (diakses pada 20 Januari 2026).

European Parliamentary Research Service (EPRS), *Greece’s Predatorgate: The Latest Chapter in Europe’s Spyware Scandal?*, Briefing Paper,

2022, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EP_RS_ATA\(2022\)733637_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EP_RS_ATA(2022)733637_EN.pdf) (diakses pada 20 Januari 2026).

Forbidden Stories, "Pegasus: The New Global Weapon for Silencing Journalists," *ForbiddenStories.org*, April 2022, <https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/> (diakses pada 20 Januari 2026).

George Packer, "How Democracies Spy on Their Citizens," *The New Yorker*, 25 April 2022, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens> (diakses pada 20 Januari 2026).

Indonesia Baik, "*Bidang Kerja 13 Komisi DPR RI Periode 2024–2029*," *Indonesiabaik.id*, 2017, <https://indonesiabaik.id/infografis/bidang-kerja-13-komisi-dpr-ri-periode-2024-2029> (diakses pada 3 Februari 2026)

Kementerian Keuangan Republik Indonesia, *Buku II Nota Keuangan Beserta Rancangan Anggaran Pendapatan dan Belanja Negara Tahun 2024*, Kemenkeu, 2024.

Kementerian Pertahanan Republik Indonesia, "Menhan RI dan RRT Perkuat Kerja Sama Strategis Bidang Pertahanan," *Kemhan*, 22 Januari 2025, <https://www.kemhan.go.id/2025/01/22/menhan-ri-dan-rrt-perkuat-kerja-sama-strategis-bidang-pertahanan.html> (diakses pada 20 Januari 2026).

Kementerian Pertahanan Republik Indonesia, "Wamenhan RI Buka Defence Technology Forum 2025, Dorong Inovasi Teknologi Pertahanan," *Kemhan*, 19 November 2025, <https://www.kemhan.go.id/2025/11/19/wamenhan-ri-buka-defence-technology-forum-2025-dorong-inovasi-teknologi-pertahanan.html> (diakses pada 20 Januari 2026).

Khatwani, Kezia, Adzkar Ahsinin, Gurnadi, Parasurama Pamungkas, dan Nurul Izmi. *Privasi dalam Rumah Kaca: Menuntut Akuntabilitas Penggunaan Spyware di Indonesia*. Jakarta: ELSAM, 2026.

LSP Pengadaan Indonesia, "Kontrak Jangka Pendek vs Jangka Panjang", *LSP Pengadaan Indonesia*, 2023, <https://lspPengadaan.id/kontrak-jangka-pendek-vs-jangka-panjang/> (diakses pada 20 Januari 2026)

MetroTVNews, "Kemhan dan KNDS Jalin Kerja Sama Strategis di Bidang Teknologi," *MetroTVNews*, 20 November 2025, <https://www.metrotvnews.com/play/bD2CMewQ-kemhan-dan-knds-jalin-kerja-sama-strategis-di-bidang-teknologi> (diakses pada 20 Januari 2026).

Organized Crime and Corruption Reporting Project (OCCRP), "Where NSO Group Came From and Why It's Just the Tip of the Iceberg," *The Pegasus*

Project, 20 Juli 2021, <https://www.occrp.org/en/project/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg> (diakses pada 20 Januari 2026).

Pieter Omtzigt, *Mass Surveillance*, Report, Doc. 13734 (Strasbourg: Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, 8 Maret 2015).

Progressive Alliance of Socialists and Democrats in the European Parliament (S&D), “Pegasus Spyware Inquiry: S&Ds Call for Strong EU Regulation to Prevent Abuse by Member States,” *Socialists and Democrats*, 14 Juni 2023, <https://www.socialistsanddemocrats.eu/newsroom/pegasus-spyware-inquiry-sds-call-strong-eu-regulation-prevent-abuse-member-states> (diakses pada 20 Januari 2026).

Regulation (EU) 2016/679 (GDPR), arts. 51–54 (Chapter VI: Independent Supervisory Authorities), OJ L 119 (4 Mei 2016).

Silvia Calderón dan Ana Gaitán, eds., *Surveillance Trends and Practices in Latin America: Case Studies from Brazil, Chile, Colombia, El Salvador, Mexico, Peru, and Paraguay* (Juni 2025).

Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie K. Pell, “It’s Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law,” *Harvard Journal of Law & Technology*, volume 30, nomor 1, 2016, halaman 2-73.

Sukarjito, “Prabowo Terima Jenderal China, Sepakat Perkuat Teknologi Militer,” *BeritaSatu*, 6 Agustus 2025, <https://www.beritasatu.com/nasional/2910998/prabowo-terima-jenderal-china-sepakat-perkuat-teknologi-militer> (diakses pada 20 Januari 2026)

Tibiko Zabar, “Waspada Ancaman Demokrasi: Awasi Penggunaan, Polri Harus Buka Informasi Pengadaan “Kuda Terbang””, *Aliansi Jurnalis Independen*, 2023, <https://aji.or.id/informasi/waspada-ancaman-demokrasi-awasi-penggunaan-polri-harus-buka-informasi-pengadaan-kuda> (diakses pada 20 Januari 2025)

United Nations Human Rights Council, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/41/35, 41st sess. 24 June–12 July 2019, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur> (diakses pada 20 Januari 2026)

VSquare.org, “Pegasus Spyware Hacking WhatsApp – Meta, Hungary, Czech Republic,” *VSquare.org*, 17 April 2025, <https://vsquare.org/pegasus-spyware-hacking-whatsapp-meta-hungary-czech-republic/> (diakses pada 20 Januari 2026).

Yusa Djuyandi, Hasya Aiman Nadhir, Afifah Amaliya Pohan, Duta Smaradana, Adisa Naura Priadi, Proses Sekuritisasi dan Desekuritisasi dalam Upaya Menurunkan Angka Kasus Covid-19 di Indonesia, *Jurnal Wacana Publik*, Volume 16, Nomor 1, 2023, halaman. 1-12.

